UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

LYDIE JORGE BATISTA

O *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA EM PROCESSO PENAL

Dissertação de Mestrado

em Ciências Jurídico-Forenses

LISBOA, 2018

UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

LYDIE JORGE BATISTA

O *MALWARE* COMO MEIO DE OBTENÇÃO DE PROVA EM PROCESSO PENAL

Dissertação de Mestrado

em Ciências Jurídico-Forenses

Orientador

Professor Doutor Paulo de Sousa Mendes

LISBOA, 2018

Quando nada parece ajudar,

eu vou e olho para o canteiro a martelar a sua pedra,

talvez cem vezes, sem que nem uma só rachadura apareça.

No entanto, na centésima primeira martelada, a pedra abre-se em duas,

e eu sei que não foi aquela que o conseguiu, mas todas as que vieram antes.

(*Jacob Riis*)

Agradecimentos

Aos meus Pais, por todo o apoio, amor e dedicação concedidos e por me permitirem fazer sempre as minhas escolhas. Não há palavras suficientes para os distinguir!

Ao meu irmão. É impossível expressar o quanto ele é importante para mim.

Ao Emanuel, por me apoiar e acompanhar nos meus sonhos e, principalmente, por não me deixar desistir deles.

À minha grande e excelente família. É difícil individualizar cada um de vós, mas agradeço-vos todo o carinho e preocupação manifestados.

À Patrícia Bernardes e à Inês Tomé, pela amizade e apoio.

Ao Professor Doutor Paulo de Sousa Mendes, pelos conselhos e críticas construtivas. Sem dúvida, os seus incentivos estimularam-me a querer ir sempre mais além.

Ao Mestre David Silva Ramalho, pela sua disponibilidade, ajuda e sugestões partilhadas.

A todos, a minha profunda gratidão, por serem o 'toque' que me permitiu chegar ao resultado final!

É que sem uma lei coerente que defina parâmetros claros, não há boas práticas que nos valham. E o pior é que elas – as leis más – conduzem ao arbítrio, e à injustiça. Ora não há pior descrédito que possa recair sobre os tribunais do que o de não conseguirem administrar justiça.

Maria de Fátima Mata-Mouros, «Escutas Telefónicas – O que não Muda com a Reforma», *Revista do CEJ*, número 9 (especial), 1.º semestre de 2008, p. 220

O que é decisivo não é tanto saber se a lei nova oferece hoje melhor solução para os problemas de ontem. Há-de prevalentemente questionar-se se ela assegura uma resposta adequada e eficaz aos problemas de hoje.

Manuel da Costa Andrade, *"Bruscamente no Verão Passado", a reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, Coimbra, Coimbra Editora, 2009, p. 27

Índice

Resumo

Com a evolução tecnológica, surgiram novas e graves formas de criminalidade e tornou-se mais difícil a deteção e prova da prática destes crimes. Em consequência, os "meios tradicionais" de investigação, essencialmente pensados para uma realidade física, viram-se insuficientes neste combate. Contudo, o progresso não pode ser exclusivamente encarado como uma ameaça, mas também como um importante desafio jurídico e tecnológico, na medida em que possibilitou o desenvolvimento e surgimento de (novos) e mais eficazes meios à disposição da investigação criminal, aptos a responderem adequadamente aos novos problemas. É precisamente neste panorama que o *malware* passou a ser visto como um potencial meio de obtenção de prova em processo penal, isto é, como uma ferramenta útil a ser utilizada pelas autoridades competentes na repressão ou mesmo na prevenção criminal. Porém, por ser um meio oculto, e devido às suas próprias potencialidades, o uso de *malware* constitui, simultaneamente, um foco de tensão entre os direitos fundamentais dos cidadãos e os princípios da investigação, prevenção criminal e descoberta da verdade material. Nesse sentido, este meio de obtenção de prova só poderá ser sólido e eficaz se tiver por base os direitos e liberdades fundamentais. Impõe-se, assim, pensar em soluções de compatibilização entre os interesses de perseguição penal e de tutela dos direitos fundamentais. Em conclusão, é verdade que este meio oculto pelas suas próprias características distintivas dos restantes pode ser extremamente útil, mas só será viável e eficaz se for necessário, proporcional e conforme com os procedimentos aplicáveis, respeitando plenamente os direitos fundamentais dos cidadãos. No que a esta matéria diz respeito, os Estados Unidos da América são um país onde a utilização de *malware* é recorrente e, por consequência, amplamente debatida. Não obstante, o seu uso é feito à custa de uma forçosa interpretação da lei. Por sua vez, na Europa, existem ordenamentos jurídicos que preveem o seu recurso. Em Portugal, temos dois grupos: os que defendem que o *malware* encontra a sua consagração na lei do cibercrime, e os que discordam desta interpretação. Ora, é precisamente em torno destas questões que a presente dissertação se desenvolverá, entre elas, a legitimidade de recurso ao *malware* em processo penal, a sua (não) previsão na lei do cibercrime e, por fim, a nossa proposta de regime jurídico.

Palavras-chave: *Malware*; Métodos Ocultos; Teoria Geral dos Métodos Ocultos; Meios de Obtenção de Prova; Lei do Cibercrime.

Abstract

With the technological evolution, new forms of crime appeared and it became more difficult to detect and prove the committing of these crimes. As a consequence, the "traditional tools" of investigation, essentially envisioned for a physical reality, were insufficient in this fight. Nevertheless, progress can not only be seen as a threat but also as a major legal and technological challenge as it has enabled the development and the emergence of (new) and more effective tools that are now available to criminal investigations, and that are capable of responding effectively to new problems. It is precisely in this context that malware became a potential tool for obtaining evidence in criminal proceedings, that is, a useful tool to be used by the competent authorities in criminal repression or even criminal prevention. However, because it is a hidden tool and because of its own potentialities, the use of malware is simultaneously a focus of tension between the fundamental rights of citizens, the principles of investigation, criminal prevention and the discovery of material truth. In this sense, this method of obtaining evidence can only be solid and effective if it is based on fundamental rights and fundamental freedoms. It is then necessary to propose solutions that are compatible with both the interests of criminal prosecution and the protection of fundamental rights. In conclusion, this tool can be extremely useful due to its own distinctive characteristics, but it will only be viable and effective if the tool is necessary, proportional and in accordance with the applicable procedures, with respect to the fundamental rights of citizens. As far as this matter is concerned, the use of malware in the United States of America is recurrent and therefore widely debated. Nevertheless, the use of malware is made through a forcible interpretation of the law. On the other hand, in Europe, there are legal frameworks that foresee its use. In Portugal, we have two groups: those who claim that malware finds its finds its place in the law of cybercrime, and those who disagree with this interpretation. However, it is precisely around these issues that the present dissertation will develop, among them, the legitimacy of using malware in criminal proceedings, its (not) prediction in the law of cybercrime and, finally, our proposal of legal framework.

***Keywords*:** *Malware*; *Covert Methods*; *General Theory of Covert Methods*; *Means of Obtaining Evidence*; *Cybercrime Law*.

Siglas e abreviaturas

AA.VV. – Vários autores

CEDH – Convenção Europeia dos Direitos do Homem

Cf. – Confrontar, ver também, referir-se a

CIPAV – *Computer and IP Address Verifier*

Cit., cits. – Citado, citada, cita-se; citação, citações

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

DUDH – Declaração Universal dos Direitos Humanos

E. g. – (*Exempli grati*) por exemplo

Et al. – (*Et alii*) e outros

FBI – *Federal Bureau of Investigation*

GG – *Grundgesetz* (Lei Fundamental/Constituição da República da Alemanha)

GPRS – *General Packet Radio Service*

GSM – *Global System for Mobile Communications*

IMEI – *International Mobile Equipment Identity*

IMSI – *International Mobile Subscriber Identity*

Infra – Abaixo

IP – *Internet Protocol*

LC – Lei do cibercrime

N.º, n.os – Número, números

NIT – *Network Investigative Technique*

Op. cit. – Da obra citada

P., pp. – Página, páginas

S., ss. – Seguinte, seguintes

StGB – *Strafgesetzbuch* (Código Penal Alemão)

StPO – *Strafprozeßordnung* (Código de Processo Penal Alemão)

Supra – Acima

TEDH – Tribunal Europeu dos Direitos do Homem

TOR – *The Onion Router*

UMTS – *Universal Mobile Telecommunication System*

V. – (*Versus*) em oposição

Modo de citar e acordo ortográfico

As citações das monografias serão feitas inicialmente por autor, título, local de publicação, data e páginas, ao passo que os artigos científicos serão por autor, título do artigo, publicação ou obra coletiva onde se encontra inserido, data e páginas.

Todas as subsequentes citações serão apenas efetuadas por referência ao autor, título e página; caso se trate de artigo, por autor, título e página.

Esta dissertação respeita as normas do Novo Acordo Ortográfico da Língua Portuguesa, que entrou em vigor em janeiro de 2009.

Introdução

Como referiu JORGE DE FIGUEIREDO DIAS[1], o processo penal é espelho do Estado e deve sê-lo das alterações que se verificam nas condições socioculturais, políticas e económicas da vida comunitária, quer no fenómeno da criminalidade quer na realidade processual. Assim, naturalmente, o progresso tecnológico e a própria evolução da sociedade têm repercussões a estes dois níveis. Por um lado, surgiram novos crimes e os tradicionais deixaram de ser exclusivamente praticados no mundo físico/material e passaram-no também a ser num mundo digital, ou seja, num espaço distinto, mas impercetível aos sentidos, portanto inexistente[2]. Por outro, os "meios tradicionais" de obtenção de prova tornaram-se insuficientes ante as dificuldades de deteção dos crimes, de obtenção de prova e das próprias características da prova digital – imaterial, frágil, volátil e dispersa[3].

Ora, as novas formas de criminalidade, como os atentados terroristas, a pornografia infantil, o tráfico de estupefacientes, armas e seres humanos, a anonimização, a criptografia[4], as dificuldades de superação e resolução dos problemas que surgiram com esta evolução, entre outros, sensibilizaram os Estados e reforçaram a necessidade de técnicas inovadoras à disposição da investigação criminal, contribuindo para introduzir outros elementos e fatores na ponderação ao recurso a métodos ocultos.

É precisamente neste contexto que surge o tema que nos propomos tratar: o *malware* como meio de obtenção de prova em processo penal. É um tema cada vez mais atual e inevitável, porque, por um lado, a cibercriminalidade é um problema crescente

---

[1] Ver, deste autor, «O Processo Penal Português: Problemas e Prospectivas», *Que Futuro Para o Direito Processual Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, coord. Mário Ferreira Monte *et al.*, Coimbra, Coimbra Editora, 2009, p. 805.

[2] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Dissertação de Mestrado em Direito, Especialidade de Ciências Jurídico-Criminais, Lisboa, Faculdade de Direito da Universidade de Lisboa, 2015, p. 20 (policopiada). Entretanto, publicada pelas Edições Almedina, Coimbra, em 2017.

[3] A este propósito ver DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., pp. 81-87.

[4] A criptografia é utilizada, entre outros fins, na proteção de dados e comunicações, logo, dificulta a investigação criminal. O Parlamento Europeu concluiu que um dos principais argumentos para a utilização das técnicas de *hacking*, nomeadamente de *malware*, é o crescente recurso a esta técnica, consubstanciando uma preocupação constante nas últimas décadas. A criptografia deu origem à designada "*Crypto Wars*", nos Estados Unidos da América, ou seja, a diversas medidas políticas do Governo norte-americano, a fim de desenvolver capacidades para decifrar todos os dados criptografados, mas também inúmeros debates internacionais. Cf. MIRJA GUTHEIL *et al.*, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, Estudo do Parlamento Europeu, Espaço de Liberdade, de Segurança e de Justiça, Bruxelas, 2017, pp. 18-21, disponível em http://www.europarl.europa.eu/thinktank/pt/document.html?reference=IPOL_STU%282017%29583137 [consultado a 25-04-2017].

na Europa, que tem vindo a aumentar em termos de intensidade, complexidade e dimensão, e em alguns países os casos de cibercrime chegam a exceder a criminalidade tradicional. Por outro, a prova digital é cada vez mais frequente e a utilização de ferramentas de encriptação e de anonimização para fins criminosos não pára de aumentar, pelo que os ataques informáticos tornam-se cada vez mais reiterados e ardilosos, recorrendo a *softwares* maliciosos superadores dos tradicionais, como é o caso do tipo *ransomware*[5].

Os meios de obtenção de prova são os instrumentos utilizados pelas autoridades competentes para investigar e recolher formas de provas, ou seja, trata-se de uma maneira de chegar à recolha de prova[6]. Através deles, podem obter-se, *e. g.*, documentos, coisas, indicação de testemunhas e, por vezes, até a próprio forma de obtenção da prova acaba por ser também um meio de prova[7]. De entre os meios, existem também os ocultos.

Historicamente, os métodos ocultos de investigação criminal não representam uma novidade. Nas palavras de MANUEL DA COSTA ANDRADE[8], a inovação destas formas clandestinas de investigação está associada, por um lado, ao seu carácter já institucionalizado, isto porque mesmo não existindo uma previsão legal é sempre possível apelar a princípios constitucionais para se utilizar a prova obtida, por outro, devido à sua generalização. Estes meios ocultos irão continuar a aumentar ao mesmo ritmo do progresso e das inovações tecnológicas.

---

[5] Tipo de *software* malicioso que restringe o acesso ao sistema informático infetado e, em consequência, só o restabelece mediante o pagamento de um resgate. Por outras palavras, trata-se de um sequestrador informático. Neste âmbito, recorde-se o ataque internacional de 12 de maio de 2017, que também afetou Portugal. Ver em http://visao.sapo.pt/actualidade/mundo/2017-05-15-O-que-precisa-de-saber-sobre-o-ciberataque-que-atingiu-mais-de-150-paises [consultada a 07-10-2017]. Cf. Relatório sobre a luta contra a cibercriminalidade [2017/2068 (INI)], número PE604.566V03-00, A8-0272/2017, da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu, de 25 de julho de 2017, p. 6, disponível em: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0272+0+DOC+PDF+V0//PT [consultado a 03-10-2017].

[6] Cf. TERESA MARIA DA SILVA BRAVO, «Revistas e Buscas: O Processo Penal na Era da Globalização», *in* Manuel Monteiro Guedes Valente (coord.), *III Congresso de Processo Penal*, Coimbra, Almedina, 2010, p. 132; ANTÓNIO DA SILVA HENRIQUES GASPAR *et al.*, *Código de Processo Penal Comentado*, Coimbra, Almedina, 2014, p. 785. (2.ª edição, 2016)

[7] Cf. Acórdão do Tribunal da Relação de Guimarães, de 29-03-2014 (Maria Augusta), processo n.º 1680/03-2, disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/926f6fea6511bf6e80256ee0003afd32?OpenDocument [consultado a 14-10-2017].

[8] Cf. MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação (*Plädoyer* para uma teoria geral)», *Que Futuro Para o Direito Processual Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, coord. Mário Ferreira Monte *et al.*, Coimbra, Coimbra Editora, 2009, pp. 531-532.

Os meios ocultos de obtenção de prova qualificam-se pela sua intromissão na vida das pessoas investigadas, sem o seu conhecimento ou consentimento. Por sua vez, as mesmas continuam a agir, interagir e comunicar natural e inocentemente, contribuindo, não raras as vezes, para a sua autoincriminação[9]. Em conclusão, os meios ocultos são caracterizados pela sua danosidade social, designadamente, devido ao sacrifício de bens jurídicos e direitos fundamentais[10].

O *malware* insere-se nos meios de obtenção prova ocultos, por ser um tipo de *software* malicioso concebido e desenvolvido com o intuito de se infiltrar no sistema informático[11] sem o conhecimento e consentimento do sujeito investigado. Permite, em consequência, o acesso a uma grande quantidade de dados e funcionalidades, sempre sem interferir com o uso normal por parte do seu utilizador.

Este meio encoberto engloba em si diversas características e capacidades de outros meios, mas também particularidades que o afastam deles e, no limite, tem potencialidades até ora desconhecidas. Assim, comparativamente com outros métodos ocultos, o *malware* tem tendência para uma maior danosidade social, grau de invasão e devassa da privacidade e violação da autodeterminação.

Consequentemente, a construção de um regime jurídico para o *malware* passará pela necessidade de equilíbrio da tensão entre a exigência, de um lado, da manutenção do processo penal como um sistema de sólida garantia dos direitos fundamentais dos cidadãos, e, de outro, o tratamento eficiente das novas formas de criminalidade[12]. Ou seja, terá que existir concordância prática entre os interesses em jogo. Por seu turno, as *guidelines* do regime jurídico devem ser bem estruturadas e pensadas, de forma a respeitar princípios como o da determinabilidade legal, necessidade e da proporcionalidade.

---

[9] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado", a reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, Coimbra, Coimbra Editora, 2009, Pp. 105-106.

[10] Cf. MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação…», op. cit., p. 536.

[11] Recorde-se, para o efeito, o conceito de "sistema informático" previsto na alínea a) do artigo 2.º da LC " *«Sistema informático», qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção*".

[12] Como já referiu JORGE DE FIGUEIREDO DIAS ainda que a propósito dos novos âmbitos problemáticos que se colocaram à legislação nos últimos tempos. «O Processo Penal Português: Problemas e Prospectivas», op. cit., p. 809.

Apesar de haver quem defenda que o *malware* encontra a sua previsão legal na LC, não acompanhamos esta interpretação. Por isso, defendemos que a sua utilização se reflete nos problemas de novação legislativa.

Acontece que, nesta matéria, em Portugal, ao contrário do que sucede na Alemanha, não existe uma teoria geral dos métodos ocultos. Os meios encobertos à disposição da investigação criminal encontram-se dispersos entre o CPP e diversas leis avulsas, motivo pelo qual se torna árduo fazer um adequado levantamento do respetivo regime jurídico, ou seja, identificar-se as categorias e definir os princípios basilares comuns a cada meio e, na prática, concretos para cada um deles. Verificam-se incoerências de regimes jurídicos, que só uma organização sistemática poderia colmatar, nomeadamente, evitando as desproporcionalidades e desalinhos verificados[13].

Em conclusão, independentemente do panorama, a verdade é que os meios ocultos, e no nosso caso o *malware*, não devem atuar ao 'negro' antes se impõe a sua utilização às 'claras', através de um regime jurídico ponderado e adequado às suas particularidades.

1. Delimitação do tema

O problema que nos propusemos tratar resulta, assim, da conjugação de duas questões essenciais: (1) pode o *malware* ser utilizado em processo penal?; e (2) com que pressupostos e limitações?

Para responder à nossa primeira questão, começaremos por apresentar as potencialidades do *malware* para, posteriormente, efetuarmos uma reflexão, ainda que não exaustiva, de interesses e direitos constitucionais, isto é, o equilíbrio entre os direitos lesados e os fundamentos para a sua utilização.

Posto isto, avançaremos para a nossa segunda discussão. Aqui, iremos analisar, se bem que não profundamente, o regime jurídico das escutas telefónicas e das ações encobertas, a fim de entender quais as variáveis subjacentes a estes meios, melhor dizendo, o catálogo de crimes, o grau de suspeita, a subsidiariedade, a autoridade competente e o procedimento. No fim, o objetivo será o de estarmos em condições de propor um regime jurídico para o *malware*.

[13] Cf. MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação…», op. cit., pp. 539-540.

2. Metodologia adotada e ordem de razão

A presente exposição está estruturada em quatro pontos fundamentais: (1) o enquadramento técnico do *malware*; (2) a sua legitimidade; (3) os eventuais pressupostos de utilização; e (4) a proposta de regime jurídico.

No primeiro capítulo, faremos uma breve contextualização da evolução legislativa em matéria de ambiente digital. Apontaremos quais os diplomas existentes e os meios ocultos de obtenção de prova à disposição da investigação criminal.

No segundo capítulo, desenvolveremos o conceito de *malware*, as suas categorias e o modo de instalação. O objetivo é demonstrar as potencialidades técnicas e a extensão deste meio encoberto.

Passaremos, de seguida, ao terceiro capítulo. Numa primeira abordagem, apresentaremos a experiência norte-americana, com o intuito de demonstrar, em termos práticos, a aplicação das capacidades e potencialidades deste meio, assim como os requisitos essências considerados pelos tribunais para a sua (não) utilização. Já numa segunda abordagem, exporemos alguns dos regimes jurídicos europeus, indicando os pressupostos para a utilização de *malware*. O propósito é efetuar um levantamento jurídico.

Chegados ao quarto capítulo, refletiremos a legitimidade do uso de *malware* perante os direitos fundamentais afetados. Pretendemos fazer uma ponderação entre as necessidades de salvaguarda do quadro constitucional de direitos, liberdades e garantias e das exigências que se colocam ao Estado e ao sistema de justiça, a nível de prevenção e repressão criminal.

No quinto capítulo, analisaremos o regime jurídico de dois meios ocultos – as escutas telefónicas e ações encobertas. Por um lado, pois consideramos que as escutas são o regime mais elaborado e aperfeiçoado que possuímos e, por outro, por as ações encobertas se assemelharem a nível de danosidade, nalguns pontos, com o *malware*. O objetivo essencial é entender o raciocínio do legislador e as variáveis utilizadas em ambos os regimes para, no fim, demonstrar que existem pressupostos comuns que devem estar sempre plasmados em qualquer regime jurídico.

Já no sexto capítulo, iremos expor as diversas interpretações sobre a previsão ou não na LC do uso de *malware*. Como somos da opinião que o *malware* ainda não tem previsão legal, iremos apresentar, no último capítulo, a nossa proposta de regime jurídico baseado nas considerações efetuadas anteriormente.

1. Breve evolução legislativa em matéria de ambiente digital

Nas duas últimas décadas, surgiram, quer a nível nacional quer internacional, diversos diplomas no âmbito da cibercriminalidade e da prova digital. Por esse motivo, a presente exposição começará por fazer uma breve evolução legislativa, indicando o âmbito e as novidades das sucessivas leis. O intuito é, nesta perspetiva, demonstrar a dispersão que atualmente se verifica em matéria de meios de obtenção de prova e, de outro ponto de vista, evidenciar a dificuldade do legislador nacional em acompanhar o progresso tecnológico e o fenómeno da criminalidade. Por fim, porque a interpretação das leis que temos não é fácil nem direta, indicaremos, não exaustivamente, quais os meios ocultos de obtenção de prova regularmente à disposição da investigação criminal.

Em Portugal, a Lei n.º 109/1991, de 17 de agosto, conhecida pela Lei da Criminalidade Informática, foi pioneira em matéria de cibercriminalidade. Por um lado, definiu, entre outros, rede informática, sistema informático, programa informático e interceção. Por outro, tipificou a falsidade informática, o dano relativo a dados ou programas informáticos, a sabotagem informática, o acesso ilegítimo, a interceção ilegítima e a reprodução ilegítima de programa protegido. Apesar de ter definido alguns conceitos e crimes informáticos, em termos procedimentais, não fez a adaptação ao mundo virtual.

Mais tarde, fruto das exigências internacionais e do próprio ambiente digital, surgiu aquele que viria a ser o mais importante trabalho internacional em matéria de crime no ciberespaço – a Convenção sobre o Cibercrime. Foi adotada, em Budapeste, a 23 de novembro de 2001, no âmbito da Conferência Internacional sobre a Cibercriminalidade, e, na sua essência, tinha três objetivos principais: criar um conjunto de infrações comuns entre os diversos Estados signatários; criar um conjunto de medidas processuais que permitissem às autoridades competentes de cada um desses Estados a recolha de prova em ambiente digital; e, por fim, estabelecer mecanismos de cooperação internacional[14].

Relativamente ao segundo objetivo, a Convenção previu essencialmente quatro tipos de procedimentos processuais penais, em matéria de criminalidade informática: (1) a conservação expedita de dados informáticos armazenados; (2) a injunção de

[14] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 49.

comunicar; (3) a busca e apreensão de dados informáticos armazenados; e (4) a recolha, em tempo real, de dados informáticos.

Por sua vez, a 24 de fevereiro 2005, nasceu a Decisão-Quadro 2005/222/JAI do Conselho da União Europeia, relativa a ataques contra os sistemas de informação, cujo principal objetivo foi a descrição de comportamentos qualificáveis como crime, a criação de normas conexas relacionadas com estes comportamentos, a criminalização da instigação, do auxílio, da cumplicidade e da tentativa, a responsabilização das pessoas coletivas, a criação de regras em matéria de competência territorial e do intercâmbio de informação[15]. Ou seja, quanto a medidas processuais, nada regulou.

Dois anos depois, em 2007, o legislador nacional procedeu à revisão do CPP. Esta revisão foi muito criticada pela doutrina[16], na medida em que ficou aquém de todas as expectativas. Esperava-se que o legislador, através dela, ultrapassasse a dispersão que se verificava nos regimes jurídicos das investigações e assumisse decisões legislativas indispensáveis à superação de ambiguidades no quadro de soluções do CPP[17]. Em matéria de meios ocultos de investigação, existiam alguns[18] que imponham ao legislador de 2007 a tarefa de regulamentação[19], todavia, esta foi uma chamada a que o legislador preferiu faltar.

Em termos procedimentais, o legislador optou por estender o regime previsto para as escutas telefónicas a outras realidades, como o correio eletrónico, a transmissão de dados via telemática, a localização celular e os registos de realização e conversações ou comunicações[20], misturando realidades técnicas diferentes e até opostas[21].

Em síntese, esta revisão contribuiu para a incerteza e para a insegurança jurídica já verificadas, dificultando a tarefa das instâncias formais de controlo[22]. Na realidade,

---

[15] Cf. Exposição de motivos da proposta de Lei n.º 289/X do Parlamento, disponível em https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=34566 [consultada a 24-10-2016].

[16] A este propósito, entre outros, vejam-se MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., JOÃO CONDE CORREIA, «Prova digital: as leis que temos e a lei que devíamos ter», *Revista do Ministério Púbico*, número 139, ano 35, julho/setembro de 2014, pp. 29-59, e PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, Coimbra, Coimbra Editora (Wolters Kluwer), 2010, pp. 87-94.

[17] Cf. MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação…», op. cit., p. 540.

[18] Entre eles, o *malware*.

[19] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 105.

[20] Como veremos mais em pormenor, no capítulo quinto.

[21] Cf. JOÃO CONDE CORREIA, «Prova digital: as leis que temos e a lei que devíamos ter», op. cit., pp. 31-32.

[22] Cf. *Ibidem*.

não contemplou normas especiais, nomeadamente para a recolha da prova digital, que por si exige regimes jurídicos autónomos.

Pouco tempo depois, em 2008, a Lei n.º 32/2008, de 17 de julho, que transpôs para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho da União Europeia, de 15 de março[23], consagrou um conjunto de normas específicas acerca da conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. Regulou também a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e coletivas, bem como dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes[24]. Ora, mais uma vez, o legislador não manteve a centralidade no CPP.

Chegados a 2009, decorridos nove anos após a assinatura da Convenção sobre o Cibercrime, o Governo Português, a 20 de maio, apresentou à Assembleia da República a Proposta de Lei n.º 289/X/4ª. O decreto da Assembleia n.º 373/X viria a aprovar a LC, que transpôs para a ordem jurídica interna a Decisão-Quadro n.º 2005/222/JAI do Conselho da União Europeia, de 24 de fevereiro de 2005, relativa a ataques contra sistemas de informação e adaptou o Direito Interno à Convenção sobre o Cibercrime do Conselho da Europa. Por fim, a 15 de setembro de 2009, foi publicada em Diário da República a Lei n.º 109/2009 (LC), que revoga a Lei da Criminalidade Informática.

Esta lei introduziu e ampliou diversos conceitos jurídico-informáticos, alargou os tipos incriminadores dos cibercrimes que antes estavam previstos na Lei da Criminalidade Informática, estabeleceu o princípio da competência universal e consagrou múltiplas medidas processuais de obtenção de prova digital e de combate ao cibercrime. Fixou ainda obrigações para as operadoras de comunicação, com o intuito de preservar a prova digital, e definiu várias medidas de cooperação internacional no que respeita à obtenção de prova digital e, genericamente, ao combate à criminalidade informática[25]. Ou seja, para o que aqui nos interessa, foram introduzidos novos e mais

---

[23] Note-se que esta Diretiva foi declarada inválida pelo Tribunal de Justiça da União Europeia. A este propósito, ver JOÃO CONDE CORREIA, «Prova digital: as leis que temos e a lei que devíamos ter», op. cit., p. 38.

[24] Cf. artigo 1.º da aludida lei.

[25] Cf. RENATO LOPES MILITÃO, «A propósito da *prova digital* no processo penal», *Revista da Ordem dos Advogados*, volume I, ano 72, janeiro/março de 2012, p. 273, disponível em https://portal.oa.pt/comunicacao/publicacoes/revista/ano-2012/ano-72-voli-jan-mar-2012/doutrina/ [consultado a 17-05-2016].

eficazes meios de investigação contra os novos fenómenos criminais no ciberespaço – como é o caso da preservação expedita de dados armazenados num sistema informático, da injunção, da pesquisa de dados informáticos, da apreensão de dados informáticos, da interceção de comunicações e das ações encobertas.

Como refere PAULO DÁ MESQUITA[26], esta lei foi uma tentativa de alteração envergonhada ao CPP. Todavia, o legislador de 2009, mais uma vez, furtou-se a um exercício de coerência legislativa, isto porque apesar da LC consagrar um verdadeiro regime geral da prova digital, este deveria ter sido centralizado no CPP, ao invés de em mais uma lei extravagante[27].

Em consequência, nas palavras de JOÃO CONDE CORREIA[28], esta lei veio acrescentar mais um nó na teia legislativa, uma vez que as disposições processuais supracitadas aplicam-se a crimes previstos na LC, aos cometidos por meio de sistema informático e aos que seja necessário proceder à recolha de prova em suporte eletrónico, isto é, a todo sistema processual penal[29].

Diante do exposto, podemos concluir que, atualmente, em matéria de prova digital e de cibercriminalidade, o intérprete e o aplicador da lei dispõem de três diplomas legais: o CPP; a Lei n.º 32/2008, de 17 de julho; e a Lei n.º 109/2009, de 15 de dezembro (LC). Porém, em termos práticos, os mesmos diplomas colocam problemas de interpretação e conjugação, criando zonas cinzentas quanto a esta matéria.

Do ponto de vista doutrinal, há quem considere que a Lei n.º 32/2008 e a LC revogaram, ainda que parcialmente, partes da norma extensiva das escutas telefónicas prevista no artigo 189.º do CPP[30].

Quanto à relação entre a LC e a Lei n.º 32/2008, existem divergências doutrinais: há quem defenda (tese minoritária)[31] que a LC revogou parte da citada Lei n.º 32/2008, subsistindo os deveres dos fornecedores de serviços e prestação desses dados, e há quem considere (tese maioritária)[32] que estas duas leis se complementam.

---

[26] Cf., deste autor, *Processo Penal, Prova e Sistema Judiciário*, op. cit., pp. 111-112.
[27] Cf. JOÃO CONDE CORREIA, «Prova digital: as leis que temos e a lei que devíamos ter», op. cit., p. 35.
[28] Cf. *Ibidem*, pp. 34-35.
[29] No mesmo sentido, PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, op. cit., p. 98.
[30] Assim, PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, op. cit., pp. 102-105, 117 e 123, e JOÃO CONDE CORREIA, «Prova digital: as leis que temos e a lei que devíamos ter», op. cit., p. 36.
[31] PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário,* op. cit., pp. 113 e 123.
[32] RENATO LOPES MILITÃO, «A propósito da *prova digital* no processo penal», op. cit., p. 275.

Pese embora a posição adotada quanto a esta questão, a verdade é que parece impossível não concluir que a teia legislativa neste âmbito é muito complexa, contribuindo para a assimetria e desigualdade das soluções legislativas e, consequentemente, para o seu indesejável insucesso prático[33]. Em cada caso concreto, haverá que se verificar o regime processual aplicável para, de seguida, se fazer a sua interpretação.

Relativamente aos meios ocultos à disposição dos órgãos de investigação criminal, atualmente existem vários, a saber: as escutas telefónicas (artigo 187.º e ss. do CPP); a localização celular (n.º 2, do artigo 189.º do CPP); a preservação expedita de dados (artigo 12.º da LC); a injunção para a apresentação ou concessão do acesso a dados (artigo 14.º da LC); a interceção de comunicações (artigo 18.º da LC); as ações encobertas (artigo 19.º da LC e Lei 101/2001, de 25 de agosto); registo de voz e imagem (artigo 6.º da Lei n.º 5/2002, de 11 de janeiro); a videovigilância (Lei n.º 1/2005, de 10 de janeiro)[34]; e o *malware* (para quem defende que se encontra previsto na LC).

Em síntese, estamos perante um verdadeiro caos legislativo, não existindo como referência uma centralidade equilibrada e alinhada. Os nossos meios ocultos de investigação criminal caracterizam-se pelas "*lacunas e descontinuidades, incongruências e inconsistências e, sobretudo, por insustentáveis contradições e assimetrias normativas, axiológicas e político-criminais*"[35].

---

[33] Cf. JOÃO CONDE CORREIA, «Prova digital: as leis que temos e a lei que devíamos ter», op. cit., p. 30.
[34] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 109.
[35] *Ibidem*. No mesmo sentido ANTÓNIO DA SILVA HENRIQUES GASPAR *et al.*, *Código de Processo Penal Comentado*, op. cit., p. 839, refere que "*não é mais do que a manifestação da incapacidade do legislador em edificar um sistema coerente, e articulado, em matéria de aplicação das tecnologias ao processo penal.*"

2. O *malware*

Para a compreensão do tema que nos propomos tratar, reveste-se de importância dedicarmos um capítulo, ainda que breve, a conceitos mais técnicos. Assim, iremos apresentar a definição de *malware*, bem como expor o seu modo de instalação.

Importa, antes de mais, esclarecer que é normal encontrarem-se diversos conceitos[36] para aludir à utilização de *malware*. Em Portugal, o conceito mais utilizado é o de busca *online* ou de cavalo de Tróia, ainda que nem sempre seja acompanhado da sua definição.

Entre a doutrina que avançou com a sua desconstrução, cite-se PAULO PINTO DE ALBUQUERQUE[37], o qual considera que a busca *online* consiste na infiltração eletrónica em sistemas informáticos, através de *software* malicioso, por exemplo cavalos de Tróia, de modo a que, em tempo real ou diferido, o investigador tenha acesso à informação que está a ser ou foi inserida nesse sistema. Por sua vez, MANUEL DA COSTA ANDRADE[38] refere que a busca *online* apesar de ser um conceito abrangente, não é rigoroso, dizendo respeito a intromissões nos sistemas informáticos através da *internet* para observação, busca, cópia, vigilância, entre outros, dos dados que se encontram no sistema em causa. Este meio aproveita-se das possibilidades oferecidas pela *internet*, recorrendo às mesmas técnicas que as utilizadas pelos *hackers*. SANTOS CABRAL[39] acompanha que as buscas *online* consistem na busca realizada informaticamente através de instrumentos instalados entre computadores. Por fim, RITA CASTANHEIRA NEVES[40] considera que nas buscas *online* cabem as buscas de suspeitos com determinadas características através do cruzamento de dados efetuados por meio do computador.

Embora não seja totalmente adequado o recurso a um conceito informático – *malware* –, para qualificar este meio oculto de obtenção de prova, preferimos fazê-lo ao invés de adotar o conceito de buscas *online* ou cavalo de Tróia.

---

[36] Em Portugal: buscas *online* ou pesquisa *online*; em Espanha: *registros remotos*; nos países anglo-saxónicos: *remote searches*; e nos Estados Unidos da América: *electronic surveillance*, *internet surveillance*, *online surveillance* ou NIT.

[37] Cf. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4.ª edição, Lisboa, Universidade Católica Editora, 2011, p. 502.

[38] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 166.

[39] Cf. ANTÓNIO DA SILVA HENRIQUES GASPAR *et al.*, *Código de Processo Penal Comentado*, op. cit., p. 835.

[40] Cf. RITA CASTANHEIRA NEVES, *As Ingerências nas Comunicações Electrónicas em Processo Penal – natureza e respetivo regime jurídico do correio eletrónico enquanto meio de obtenção de prova*, Coimbra, Coimbra Editora (Wolters Kluwer), 2011, pp. 96-97.

Neste sentido, acompanhamos a argumentação utilizada por DAVID SILVA RAMALHO[41], quando refere que, por um lado, ao recorrermos ao conceito de busca *online* estamos desde logo a restringir o seu âmbito de aplicação e as suas potencialidades, e, por outro, estamos a adotar um conceito existente[42] a um meio que, *per si*, merece um termo novo no plano jurídico, devido às suas características.

Em síntese, o *malware* não pode ser encarado como uma busca no sentido do n.º 2 do artigo 174.º do CPP, porque, no caso de estarmos a aceder a um sistema informático fora do espaço domiciliar – como acontece com os portáteis, telemóveis ou *tablets* que se utilizam em qualquer local –, correríamos o risco de este meio ser utilizado sem a proteção jurídica que é dada às buscas domiciliárias, por estarmos fora do domicílio. Por sua vez, o *malware* além de permitir a busca ao próprio sistema, também possibilita a monitorização em direto do utilizador daquele sistema, por exemplo, através da ativação da *webcam*. Por fim, o termo "*online*" também não é o mais correto, porquanto a utilização de *malware* não implica a sua instalação ou utilização *online*, isto é, através da *internet*, como se demonstrará.

Já relativamente ao uso do conceito de "cavalo de Tróia" tecnicamente é incorreto, pois estaríamos a limitar este meio à utilização de um tipo específico de *software* malicioso.

Face ao exposto, optámos por utilizar na presente exposição, em rigor, a expressão *malware*, para não comparar este meio a outros já previstos na lei e, consequentemente, não desviar logo de início a sua carga valorativa.

2.1 Conceitos

O conceito *malware* surge da conjugação entre o adjetivo "malicioso" e o substantivo "*software*", ou seja, é um dispositivo especialmente criado para se infiltrar ou danificar um sistema informático sem conhecimento nem consentimento do seu

---

[41] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., pp. 283-287, e ID., «O uso de *malware* como meio de obtenção de prova em processo penal», *Revista de Concorrência e Regulação*, número 16, ano IV, outubro/dezembro de 2013, pp. 199-201.

[42] Como refere RITA CASTANHEIRA NEVES, *As Ingerências nas Comunicações*…, op. cit., p. 99, o advento das novas tecnologias arrastou consigo novas fórmulas que "*foram reconduzidas aos meios de obtenção de prova já existentes no Código de Processo Penal: exames, revistas e buscas, apreensões e escutas telefónicas.*" Adiantando MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., pp. 164-165, um ótimo exemplo disso é quando estamos perante a voz sobre IP (VoIP), nomeadamente através do recurso ao *software Skype.* A interceção da comunicação, enquanto circula na *internet*, é na realidade impossível, por isso, procura-se recorrer à vigilância nas fontes, captando as palavras do emitente, antes que as mesmas sejam codificadas, ou as do destinatário, depois de descodificadas. A técnica utilizada é o recurso ao *malware*, no entanto, a doutrina e a jurisprudência equiparam este procedimento a uma forma de intromissão nas telecomunicações.

proprietário[43]. Em síntese, define-se como um "*conjunto de instruções executadas no computador que levam o sistema a fazer algo que um atacante quer que ele faça*". É "*um programa simples ou autorreplicativo que discretamente se instala num sistema de processamento de dados sem o conhecimento ou consentimento do utilizador, com vista a colocar em perigo a confidencialidade dos dados, a integridade dos dados e a disponibilidade do sistema ou para assegurar que o utilizador seja incriminado por um crime informático*"[44].

Por outras palavras, o *malware* é um *software*, aparentemente inofensivo que, no fim de instalado num determinado sistema informático, permite ao 'atacante' aceder à informação nele contida, monitorizar a sua atividade, desativar ou ativar as funcionalidades de *hardware* e apropriar-se, eliminar e/ou alterar dados informáticos.

Existem vários tipos de *malware*[45], isto é, vários géneros de *softwares* que podem ser instalados e utilizados secretamente e sem autorização do seu utilizador, de modo a comprometer as funções do sistema informático. Todavia, como refere SUSAN W. BRENNER, vulgarmente apenas são conhecidos os vírus e os *worms*[46]. Tanto estes como os cavalos de Tróia são uma ponta do *iceberg*, uma vez que existem muitos mais. É a este conjunto de programas que designamos de "*malware*".

Apesar de não ser consensual nem a definição, nem as especificidades e limites de cada tipo de *software*, na presente exposição optámos por agrupar o *malware* em nove categorias: (1) cavalos de Tróia; (2) *logic bombs*; (3) *spyware*; (4) *keylogger* e *screenlogger*; (5) *rootkits*; (6) vírus; (7) *worms*; (8) *blended threats*; e (9) *bots*. Refira-se que todos estes tipos de *malware* estão aptos a serem utilizados, em abstrato, no âmbito da investigação criminal.

---

[43] Cf. SUSAN W. BRENNER, *Cybercrime and the law, challenges, issues, and outcomes*, Boston, Northeastern University Press, 2012, p. 36.
[44] Cf. DAVID SILVA RAMALHO, «O uso de *malware*…» op. cit., pp. 201-202.
[45] Cf. SUSAN W. BRENNER, *Cybercrime and the law*…, op. cit., p. 36.
[46] Como já referido, alguma doutrina quando se refere ao *malware* faz apenas referência a cavalos de Tróia ou a *trojans*. Assim, MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 165, e PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (4.ª edição), p. 502.

2.1.1 Cavalos de Tróia

Este tipo de *software* malicioso começou a ser divulgado, sobretudo no final dos anos 1990, com o famoso *Backdoor BackOrifice*, lançado pelo grupo de *hackers* intitulado de "*Cult Of the Dead Cow*"[47].

Os cavalos de Tróia são aparentemente inofensivos, mas contêm uma função oculta[48]. Este tipo de programa pode estar inserido quer num *software* quer num anexo de *e-mail* ou num *website*. Por serem aparentemente inofensivos, eles induzem o visado à sua instalação através de *download*, permitindo, automaticamente, que seja instalado no sistema informático, facilitando, assim, o seu ataque remoto.

O principal objetivo dos cavalos de Tróia é a criação de *backdoors*[49] no sistema informático infetado, ou seja, uma forma escondida de aceder remotamente ao sistema, contornando os mecanismos de autenticação existentes.

Após a sua instalação, o 'atacante' tem acesso a um vasto conjunto de informações do utilizador, desde credenciais das páginas de acesso reservado (*webmails*, redes sociais, entre outros) à captação de informação, como por exemplo, números de cartões de crédito. O 'atacante' pode ainda, danificar o sistema, instalar outros *malwares* ou mesmo navegar na *internet* de forma anónima, enviado informações através do sistema informático.

2.1.2 Logic bombs

As *logic bombs* são uma modalidade de *malware* não replicativo. Tal como o nome indica, são uma espécie de bomba sob forma de programa que fica instalado na memória do sistema informático à espera de ser ativada com a realização de uma ação ou o estado do mesmo[50].

O exemplo avançado por ERIC FILIOL[51] refere-se ao caso de um sujeito instalar este programa no seu sistema informático, programando-o para confirmar, diariamente, se o seu nome se encontra no registo da contabilidade. No momento em que este deixar

---

[47] Cf. Xmco Partners, «Les Federal Trojans», *L'ActuSécu*, número 21, 2008, p. 4, disponível em http://www.xmco.fr/actu-secu/XMCO-ActuSecu-21-FederalTrojan.pdf [consultado a 16-05-2015].
[48] Cf. JONATHAN CLOUGH, *Principles of Cybercrime*, Cambridge, Cambridge University Press, 2010, p. 34. (2.ª edição, 2015)
[49] Um *backdoor* é um recurso utilizado em diversos tipos de *malwares* para garantir o acesso remoto ao sistema infetado, explorando falhas existentes em programas instalados, em *softwares* desatualizados e em *firewall*.
[50] Cf. JONATHAN CLOUGH, *Principles of Cybercrime*, op. cit., p. 33.
[51] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 289.

de constar, o *malware*, que se encontrava inativo, aciona-se automaticamente, cifrando os documentos da empresa, inclusive os *back-ups*, com uma chave secreta, e tornando-os potencialmente indecifráveis[52].

2.1.3 Spyware

Segundo JONATHAN CLOUGH[53], o *spyware* é uma descrição genérica para um conjunto de programas que monitorizam o uso do sistema informático.

Esses *softwares* mudam consoante o *adware*[54] gerador dos *pop-ups* que recolhem as informações, as atividades e os hábitos do usuário na *internet*. Posteriormente, sem o conhecimento nem o consentimento do utilizador, transmitem estes dados a uma entidade externa.

Estes géneros de *softwares* incluem programas "*sniffer*"[55] que intercetam senhas, "*keyloggers*" que registam as teclas pressionadas pelo usuário, "*cookies*" que registam as visualizações habituais do utilizador na *internet*, e "*bugs web*" que são incorporados em páginas de *web* ou de *e-mail* e recolhem informações sobre a data/hora de acesso, endereço IP e tipo de navegador do sistema informático acedido[56].

Em suma, o *spyware* é um *software* que pode ser malicioso[57], permitindo, neste caso, espiar as ações do utilizador no sistema informático e recolher essa informação.

2.1.4 Keylogger e screenlogger

O *keylogger* é um programa-espião que regista tudo o que é digitado pelo utilizador, ou seja, é um *software* que grava e reenvia a informação digitada nas teclas do sistema informático, a fim de controlar e arquivar a atividade que foi desenvolvida, bem como obter palavras-passe.

Por sua vez, o *screenlogger* é uma forma avançada de *keylogger*, capaz de capturar a posição do cursor do rato e a tela apresentada no monitor, no momento em que é feito *click* no rato.

---

[52] Cf. DAVID SILVA RAMALHO, «O uso de *malware*...», op. cit., pp. 203-204.
[53] Cf. JONATHAN CLOUGH, *Principles of Cybercrime*, op. cit., p. 36.
[54] *Adware* designa todo o programa de computador que execute e exiba automaticamente uma grande quantidade de anúncios sem a permissão do usuário.
[55] Utilizados para intercetar os pacotes de dados que fluem da rede.
[56] Cf. JONATHAN CLOUGH, *Principles of Cybercrime*, op. cit., p. 36.
[57] Por vezes, apenas é utilizado para fins publicitários.

2.1.5 Rootkits

Os *rootkits* são um tipo de *software* que permite mascarar a presença do 'atacante', obtendo, assim, acesso privilegiado ao sistema informático[58]. Ou seja, o termo *rootkits* define o conjunto de técnicas e 'truques' que permitem esconder a presença do *backdoor* no sistema informático do visado. Estas técnicas aproveitam-se de uma vulnerabilidade do próprio sistema ou da descoberta de uma palavra-passe e, em consequência, permitem ao 'atacante' aceder como administrador ao sistema informático.

Este tipo de *malware* é utilizado, geralmente, para esconder outros tipos de *softwares* maliciosos. A técnica mais simples consiste, num sistema "Unix", em modificar o código comercial "ps" e "netstat", para não revelar o processo malicioso e as conexões de rede causadas pelo *backdoor*[59].

2.1.6 Vírus

Os vírus podem ser comparados com os vírus humanos, porque são um programa que é capaz de se propagar através dos sistemas informáticos[60].

Os vírus infetam o sistema informático, fazem uma cópia de si e utilizam esse mesmo sistema como hóspede para se multiplicar entre outros sistemas, com intuito de danificar, corromper, apagar ou alterar dados, ou mesmo instalar outro tipo de *malware*[61].

2.1.7 Worms

Tal como os vírus, os *worms* também são um programa autorreplicativo. Contudo, eles não necessitam de um hóspede ou da ajuda humana para se espalharem, na medida em que são um *software* autónomo[62].

Os *worms* recorrem à *network* para enviar cópias deles mesmos a outros sistemas na rede[63]. Por exemplo, através de *e-mails*, são enviados automaticamente para os contatos do proprietário do sistema. Podem também difundir-se pelas redes

---

[58] Cf. SUSAN W. BRENNER, «*At Light Speed*: Attribution and Response to Cybercrime/Terrorism/Warfare», *Journal of Criminal Law and Criminology*, volume 97, tomo 2, 2007, p. 380.
[59] Cf. Xmco Partners, «Les Federal Trojans», op. cit., p. 4.
[60] Cf. SUSAN W. BRENNER, *Cybercrime and the law*…, op. cit., p. 36.
[61] Cf. DAVID SILVA RAMALHO, «O uso de *malware*...», op. cit., p. 204.
[62] Cf. JONATHAN CLOUGH, *Principles of Cybercrime*, op. cit., p. 33, e SUSAN W. BRENNER *Cybercrime and the law*…, op. cit., p. 37.
[63] Cf. SUSAN W. BRENNER, *Cybercrime and the law*…, op. cit., p. 37.

GSM/GPRS/UMTS e *bluetooth*[64]. A sua propagação é feita através da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados nos sistemas informáticos. O principal objetivo é infetar, destruir dados e tornar ineficaz o próprio sistema.

2.1.8 Blended threats

Os *blended threats* são um tipo misto de *malware*, isto é, podem incluir mais do que um tipo de *software* malicioso. Nesta tipologia, temos os *spy-phishing*, que se caracterizam por ser um ataque de *phishing*[65], o qual se pode conjugar com os cavalos de Tróia ou *spyware*, com o objetivo de alcançar informação confidencial.

2.1.9 Bots

Os *bots* são um tipo de programa que infetam o sistema informático alvo e permitem que o mesmo seja controlado remotamente. O 'atacante' explora as falhas de segurança, geralmente de um sistema informático conectado à *internet*, para instalar pequenos programas designados de "*daemons*"[66] que funcionam sem o conhecimento do utilizador do sistema[67].

Além de poderem incluir funcionalidades dos *worms*, os *bots* dispõem também de mecanismos de comunicação com o 'atacante', permitindo que o programa seja controlado remotamente. O 'atacante' ao comunicar com o *bot*, pode instruí-lo a deferir ataques a outros sistemas, recolher dados e enviar *spam*, entre outros.

2.2 Modo de instalação

O *malware* pode ser instalado de diversas formas, consoante o tipo de *software* a que se refere. No essencial, existem três modelos: (1) via suporte removível; (2) via *web browser*; e (3) via *download* voluntário.

O primeiro modelo é o mais tradicional e, como o próprio nome indica, recorre a dispositivos removíveis como sejam disquetes, CD's, *pen*'*s drive* USB, discos externos, entre outros suportes destinados a serem fisicamente conectados a sistemas

---

[64] Cf. DAVID SILVA RAMALHO, «O uso de *malware*…», op. cit., p. 205.
[65] O *phishing* é a técnica que cria, por exemplo, uma página falsa de um banco ou de uma rede social, com intuito de adquirir dados pessoais financeiros, como números de cartões de crédito e senhas ou a palavra-passe e *username/e-mail*, no caso das redes sociais.
[66] *Daemons* é um programa de computador que funciona como um processo em plano de fundo, ao invés de estar sobre o controle direto do usuário.
[67] Cf. JONATHAN CLOUGH, *Principles of Cybercrime*, op. cit., p. 35.

informáticos. O que o distingue dos restantes é o facto de o *malware* utilizado ser autorreplicativo, ou seja, em geral, são vírus e *worms*.

A vantagem da utilização deste modelo para a investigação criminal prende-se com o facto de apenas o visado ser infetado com o *malware*. Esta questão é uma das principais preocupações no que concerne à utilização deste meio oculto de investigação em matéria de processo penal. É muito importante garantir que apenas a pessoa visada é infetada, evitando a possibilidade de terceiras pessoas independentes da ação serem também alvo dessa técnica maliciosa.

O segundo modelo apresenta-se, genericamente, como uma página *web*, dissimulada, que contém um código malicioso que deteta as vulnerabilidades ou configurações deficientes do sistema informático em causa.

O utilizador ao aceder a esse género de páginas irá automaticamente permitir que o *malware* se aproveite das falhas do seu sistema, infetando-o e, em consequência, o 'atacante' acaba por aceder ao seu sistema informático. Uma outra possibilidade de infeção é o caso de o utilizador clicar num determinado *link*, fazendo *download* automaticamente de *malware*.

Uma das desvantagens deste modelo, ao contrário do anterior, é que o mesmo não garante, no âmbito de uma investigação criminal, que a pessoa visada seja a única infetada, permitindo que terceiras pessoas sejam também contaminadas.

Por último, existe o modelo de infeção via *download* voluntário, isto é, através do *download* de um ficheiro específico. Instalado o *malware*, este irá procurar desativar o antivírus ou substituir-se a um programa normalmente em execução.

Este modelo poderá ter as mesmas fragilidades que o segundo acima referido, visto que terceiras pessoas também podem fazer *download* do *software* malicioso.

Em suma, existem vários tipos de *malware* que podem ser utilizados para fins de investigação criminal. No entanto, um *software* malicioso com a finalidade de ser um meio de obtenção de prova deve ser criado e estruturado com determinadas características, ajustando-se aos fins da investigação ou prevenção criminal.

Deverá o legislador, na redação da norma que preveja a utilização deste meio encoberto, definir em que consiste a técnica, de modo a não deixar ao livre-arbítrio do órgão que investiga. Em síntese, a norma deverá prever as funcionalidades e particularidades do *malware* a ser utilizado.

Como veremos no capítulo seguinte, em Itália, o Projeto de Lei Quintarelli prevê a existência de dois tipos de técnicas: as que permitem uma cópia, total ou parcial, das unidades de memória do sistema informático visado, e as que permitem a intercetação das informações dos microfones, da *webcam*, do teclado, entre outros. Acresce ainda que os *softwares* maliciosos à disposição da investigação criminal devem ser revistos anualmente por uma entidade competente, a fim de se certificarem das suas funções e de garantirem o cumprimento da lei.

Por fim, o regime jurídico deve refletir a forma de instalação do *malware*, de molde a proteger terceiros sistemas informáticos de serem infetados por técnicas semelhantes.

3. O uso de *malware* no direito estrangeiro

Após a abordagem dos conceitos mais técnicos, estamos em condições de passar à análise de alguns casos reais. A razão de ciência deste capítulo é demonstrar as potencialidades deste meio oculto no âmbito da investigação criminal, mas também o modo de funcionamento e os eventuais problemas inerentes.

Antes de desenvolvermos os casos escolhidos, faremos uma passagem por alguns mais antigos, com o intuito de demonstrar que esta técnica não é uma novidade e tem sido utilizada durante as últimas quase duas décadas (*off the record*) pelos órgãos de investigação criminal, sem a existência de um enquadramento jurídico específico.

Finda esta introdução, debruçar-nos-emos em três casos da experiência norte-americana[68]. Para além dos critérios de escolha que iremos referir de seguida, foi determinante a existência de decisões públicas[69].

O primeiro caso apresentado é um dos mais conhecidos, onde se demonstra a importância do uso de *malware* quando estão em causa ficheiros encriptados, ou seja, quando é impossível o acesso aos mesmos sem conhecimento da sua palavra-passe. Dito de outro modo, o caso em apreço demonstra na sua plenitude a importância do uso de *malware* para a superação dos problemas da criptografia. Acresce também o facto de estarmos perante um *keylogger* que foi instalado fisicamente, sem acesso à *internet*, com a garantia que aquele sistema informático seria o único infetado.

O segundo caso consiste no indeferimento de um mandado para uso de *malware*. Escolhemos o mesmo pela fundamentação utilizada, nomeadamente, a ponderação feita com a preocupação pelos direitos fundamentais.

Por último, o terceiro caso diz respeito a uma das maiores operações realizadas nos últimos anos[70], pela sua extensão, duração e complexidade. A análise do mesmo permite demonstrar as várias formas e contextos em que o *malware* pode ser utilizado, a

---

[68] Salientamos que o uso de *malware* não tem ainda enquadramento jurídico nos Estados Unidos da América. A autorização para o uso desta técnica em investigações é feita ao abrigo do regime aplicável às buscas e apreensões constantes no artigo 41.º do *Federal Rules of Criminal Procedure*. Cf. MIRJA GUTHEIL *et al.*, *Legal Frameworks for*…, op. cit., pp. 121-125.

[69] Optámos por apresentar decisões dos tribunais norte-americanos em que a informação é pública. Embora existam notícias/artigos de casos de utilização de *malware* noutros países, nomeadamente na Europa, não os trouxemos à colação uma vez que a informação não está publicada e basear-se-ia apenas em notícias de jornais e *websites online*.

[70] Durante a elaboração da dissertação foi noticiada a detenção de mil pedófilos, após a instalação de *malware* no site "The Playpen", por parte do FBI, fazendo com que esta passe a ser a maior detenção, até à presente data. Cf. «Mil pedófilos detidos depois de o FBI piratear um fórum da "darknet"», *Visão*, 05-05-2017, disponível em http://visao.sapo.pt/actualidade/sociedade/2017-05-05-Mil-pedofilos-detidos-depois-de-o-FBI-piratear-um-forum-da-darknet [consultada a 06-05-2017].

necessidade de articular a investigação com outros países e a importância da cadeia de custódia.

Posto isto, debruçar-nos-emos numa análise mais técnica, isto é, efetuaremos um breve estudo de seis regimes jurídicos europeus que preveem a utilização de *malware* como meio de obtenção de prova em processo penal.

3.1 A experiência dos Estados Unidos da América

Como referido ao longo dos últimos anos, surgiram vários casos em que se recorreu ao uso do *malware* como meio de obtenção de prova[71]. Esta matéria, desde o caso do Nicodemo S. Scarfo (1999), passando pelo *Magic Latern* (2001), aos casos do CIPAV (2007), *Timberlinebombinfo* (2007) e, mais recentemente, da Operação *Torpedo* (2011-2014), tem sido discutida pelos tribunais, debatida pela doutrina, divulgada pelos meios de comunicação social e contestada por vários ativistas e grupos[72].

Em 2001, o Governo norte-americano desenvolveu um *backdoor*, denominado de *Magic Latern,* para fins de investigação criminal no FBI. Caracterizava-se por ser um *keylogger* que se podia instalar clandestinamente ou remotamente via *internet* no sistema informático do visado. Esta técnica recorreu ao antigo "*Carnivore*", um programa *sniffer* que permitia ao agente a inserção de *software* malicioso no computador do visado, para posterior obtenção de palavras-chave de ficheiros encriptados. A instalação deste *software* poderia ser feita quer através da abertura no computador do visado de anexos de *e-mail* quer por via da exploração de vulnerabilidades no sistema operativo em causa.

O caso da utilização do *Magic Latern* revestiu a forma de um programa executável, enviado pelo FBI via *e-mail*, permitindo registar as teclas pressionadas pelo utilizador através do *keylogger*[73].

Após o surgimento do *Magic Latern*, o FBI continuou a desenvolver o conceito de "*malware* federal", nomeadamente com o *software* CIPAV, que se tornou publicamente conhecido devido ao caso *Timberlinebombinfo*[74].

---

[71] Cf. JUAN CARLOS ORTIZ PRADILLO, «El *Remote Forensic Software* como Herramienta de Investigación contra el Terrorismo», *ENAC*, número 4, outubro de 2009, pp. 3-4, disponível em http://www.academia.edu/7669471/remote_forensic_software_e_investigaci%C3%B3n_policial_en_Espa%C3%B1a [consultado a 27-04-2016].

[72] Sobre estes casos, ver KEVIN POULSEN, «FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats», *WIRED*, 18-07-2007, disponível em https://www.wired.com/2007/07/fbi-spyware/ [consultado a 09-10-2016].

[73] Cf. «Magic Lantern on back of Carnivore», *Computer Fraud & Security*, volume 2002, tomo 1, janeiro de 2002, pp. 2-3.

O CIPAV foi um *software* criado e desenvolvido para se infiltrar num computador visado e recolher uma grande quantidade de dados que, posteriormente, seriam enviados para um servidor do FBI localizado no leste da Virgínia, Estados Unidos da América.

Este tipo de *malware* era capaz de descobrir o endereço IP e MAC do visado e a sua localização, fornecer uma lista de programas em execução num determinado momento, o tipo de sistema operativo utilizado, a sua versão e número de série, o navegador de *internet* predefinido e a sua versão, o proprietário registado do computador, a conta do utilizador que se encontrava aberta e o último *website* visitado[75].

Esta técnica foi utilizada em diversos casos, entre 2001 e 2007, porém, só foram tornados públicos em 2007 com o referido processo *Timberlinebombinfo*[76]. Ao abrigo do *Freedom of Information Act* (FOIA), o FBI divulgou informações detalhadas sobre o modo de funcionamento, bem como o enquadramento legal do CIPAV[77]. No que diz respeito aos requisitos legais para a sua admissibilidade, existiam dois blocos distintos: (1) os que defendiam a desnecessidade de qualquer formalidade prévia; e (2) os que defendiam que tal utilização necessitava de autorização judicial.

Em suma, o recurso a estes meios de obtenção de prova não é uma novidade[78]. Todavia, o facto é que o seu uso, como refere MANUEL DA COSTA ANDRADE[79],

---

[74] Este caso reporta-se a 4 de junho de 2007, quando o liceu Timberline, em Idaho, nos Estados Unidos da América, recebeu do endereço dougbrigs@gmail.com várias ameaças de bomba. Numa primeira fase, o FBI tentou localizar a proveniência do endereço IP, solicitando ao *Google* e ao *MySpace* que fornecessem os *logs* registados aquando da criação do referido *e-mail*. Estes *logs* revelaram que o endereço IP utilizado era de um computador virtual localizado em Itália. Foi nestas circunstâncias que o FBI decidiu utilizar o CIPAV para descobrir o endereço IP real daquela pessoa. O CIPAV foi inserido secretamente na conta *MySpace* daquele utilizador e quando o mesmo acedeu ao seu perfil este instalou-se no computador e enviou o endereço IP real aos agentes FBI. Cf. BRIAN L. OWSLEY, «Beware of Government Agents Bearing Trojan Horses», *Akron Law Review*, volume 48, tomo 2, 2015, pp. 324-328.

[75] Cf. KEVIN POULSEN, «Documents: FBI Spyware Has Been Snaring Extortionists, Hackers For Years», *WIRED*, 16-04-2009, disponível em https://www.wired.com/2009/04/fbi-spyware-pro/ [consultado a 13-11-2016].

[76] Nomeadamente, em 2004, foi utilizado no caso de Danny Kelly, um engenheiro de Massachusetts, que cortou o acesso telefónico e o serviço de televisão por cabo a milhares de habitantes de Boston; do *hacker* que penetrou em milhares de computadores da CISCO, de vários laboratórios nacionais norte-americanos e do Laboratório de Propulsão a Jato da NASA, em 2005; em 2006, foi utilizado no caso de um *hacker* que acedeu à conta *Hotmail* de um utilizador e apoderou-se das suas informações pessoais, tentando extorquir cerca de US $ 10.000. Para mais informações sobre estes e outros casos, consultar KEVIN POULSEN, «Documents: FBI Spyware…», op. cit.

[77] Para acesso completo a esta informação, consultar JENNIFER LYNCH, «New FBI Documents Provide Details on Government's Surveillance Spyware», *Electronic Frontier Foundation*, 29-04-2011, disponível em https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav [consultado a 13-11-2016].

[78] Existem notícias de que, no ano de 2011, a polícia alemã já utilizava um *malware* denominado de *Quellen-TKÜ*. Cf. GUILLAUME CHAMPEAU, «Des failles sur le mouchard informatique de la police

vai decorrendo à margem da ilegalidade, sendo poucos os casos públicos sobre a sua utilização.

3.1.1 United States v. Nicodemo S. Scarfo and Frank Paolercio

A 15 de janeiro de 1999, em Nova Jérsia, os agentes do FBI efetuaram uma busca ao escritório de Nicodemos S. Scarfo e de Frank Paolercio, conhecidos membros de uma organização mafiosa, com objetivo de recolher meios de prova relacionados com uma operação de jogo ilegal e agiotagem. No decorrer dessa busca, os agentes efetuaram um exame ao computador dos suspeitos e ao seu disco rígido, verificando que o mesmo continha um ficheiro informático intitulado de "*Factors*", bem como um *modem* instalado. O referido ficheiro estava cifrado com o *software Pretty Good Privacy* (PGP)[80], pelo que era indecifrável sem a obtenção da sua palavra-passe.

Havendo sérios motivos para acreditar que aquele ficheiro encerrava informações com elevado valor probatório, os agentes do FBI solicitaram a emissão de dois mandados judiciais[81]: o primeiro, para aceder ao local; e, o segundo, para aceder ao sistema informático e instalar *malware*[82] por um período máximo de 60 dias.

Em maio de 1999, os agentes do FBI regressaram ao escritório dos suspeitos e instalaram secretamente no aludido computador (algures entre o teclado e o computador) um sistema de *hardware*/*software* e *firmware*, denominado de *Key Logger*

---

allemande», *Numerama*, 10-10-2011, disponível em http://www.numerama.com/magazine/20112-des-failles-sur-le-mouchard-informatique-de-la-police-allemande.html [consultado a 09-10-2016]. Em 2012, também foi noticiada a utilização de *malware* por parte da polícia alemã que permitia o acesso ao *e-mail*, *Skype* e *Facebook*. Cf. JULIEN LAUSSON, «Le mouchard de la police allemande vise aussi Skype, Gmail, Facebook …», *Numerama*, 10-10-2012, disponível em http://www.numerama.com/magazine/23989-le-mouchard-de-la-police-allemande-vise-aussi-skype-gmail-facebook.html [consultado a 11-10-2016].

[79] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 109.

[80] O PGP é um programa comercial de criptografia, criado em 1991. Na data dos factos, o programa após instalado no computador permitia a configuração de diferentes algoritmos de criptografia, como por exemplo DES (*Data Encryption Standard*), Triple DES e IDEA. Um indivíduo que recorria a este programa podia encriptar os seus ficheiros de texto, armazenar esses arquivos e desencriptá-los inserindo a palavra-passe. Assim, apenas quem tinha conhecimento da palavra-passe do arquivo é que podia aceder à informação encriptada. Cf. relatório do agente do FBI, Randall Murch, disponível em https://epic.org/crypto/scarfo/murch_aff.pdf [consultado a 30-10-2016].

[81] Os mesmos foram emitidos pelo juiz G. Donald Haneke, em 8 de maio de 1999.

[82] Cf. ANGELA MURPHY, «Cracking the Code to Privacy: How Far Can the FBI Go?», *Duke Law & Technology Review*, volume 1, tomo 1, janeiro de 2002, p. 1, disponível em http://scholarship.law.duke.edu/dltr/vol1/iss1/44/ [consultado a 15-05-2015].

System (KLS)[83], que se caracterizava por ser um *malware* do tipo *keylogger*, ainda que se tratasse simultaneamente de um *hardware*.

A função deste sistema era a de registar as teclas digitadas no computador, a fim de obter a palavra-passe necessária para decifrar o ficheiro referido, mas sempre que o *modem* estivesse desligado[84], ou seja, estando ligado não era possível registar as teclas pressionadas.

Como o KLS não funcionava em ligação à *internet*, os agentes do FBI estavam autorizados por via do supracitado mandado a entrar no escritório as vezes necessárias para recolher as informações captadas pelo *hardware*. A 23 de maio de 1999, 14 dias após a sua instalação, o KLS registou a palavra-chave do *software* PGP (o número de identificação prisional do pai de Scarfo), a qual foi recolhida em junho de 1999.

A 21 de junho de 2000, os suspeitos foram acusados pela prática dos crimes de jogo e agiotagem. No decorrer do processo, o tribunal ordenou que fosse feita uma breve apresentação do sistema KLS[85]. O agente do FBI, Randall Murch, fez um resumo, não detalhado, de como funcionava o KLS para que os suspeitos pudessem apresentar a sua defesa[86].

A defesa[87] suscitou questões de inadmissibilidade da prova, alegando que: (1) o mandado apenas autorizava a recolha de informação relativa à palavra-passe. Contudo, este *hardware* recolheu toda a informação que foi digitada no teclado, o que transformava este meio numa violação da quarta Adenda à Constituição Norte-Americana; (2) apenas foi facultado o resumo das funcionalidades do KLS em violação do procedente estabelecido pelo caso *Jencks* v. *United States*, estando a acusação obrigada a revelar as declarações das testemunhas, prestadas antes da sua inquirição em julgamento, relacionadas com o teor do seu depoimento; e (3) o KLS permitiu a interceção de comunicações dos suspeitos.

No que se refere ao segundo argumento, o tribunal afastou-o de imediato, uma vez que este procedente não encontrava paralelo com o caso *sub judice*. Quanto ao terceiro argumento, o tribunal distrital de Nova Jérsia confirmou que, apesar de alguns

---

[83] O escritório do FBI de Newark solicitou a ajuda do laboratório do FBI. Em resposta, os engenheiros configuraram um *hardware*/*software* e desenvolveram um *firmware* que permitia ao FBI obter a palavra-passe e a informação relacionada com esta. O KLS foi criado pelo FBI e era da sua exclusiva propriedade.
[84] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 280 e o relatório do agente do FBI Randall Murch, op. cit.
[85] Cf. DECLAN MCCULLAGH, «How Far Can FBI Spying Go?», *WIRED*, 31-07-2001, disponível em https://wired.com/2001/07/how-far-can-fbi-spying-go/ [consultado a 09-10-2016].
[86] Disponível em https://epic.org/crypto/scarfo/murch_aff.pdf [consultado a 30-10-2016].
[87] Disponível em https://epic.org/crypto/scarfo/supp_suppress_mot.pdf [consultado a 30-10-2016].

pormenores técnicos do KLS serem matéria confidencial, a informação prestada era no sentido de que nenhuma comunicação foi intercetada. Por esta razão, não foi dado provimento à defesa.

3.1.2 United State v. Search Warrant

Em 2013, John Doe, um cidadão residente no Texas, foi alvo de um acesso ilegítimo à sua conta de *e-mail* e, consequentemente, à sua conta bancária, a partir de um IP localizado fora dos Estados Unidos da América. Mesmo após ter tomado as devidas medidas de segurança, um *e-mail* idêntico ao seu (diferente apenas numa letra) foi criado e utilizado para enviar uma ordem de transferência do seu banco para uma conta num banco estrangeiro.

O FBI iniciou a investigação e solicitou à divisão de Houston do tribunal de distrito do Texas a emissão de um mandado judicial para a instalação de um *malware* no computador do suspeito.

O pedido explicava que após a instalação deste *malware*, o FBI poderia aceder ao disco rígido do computador, aceder à memória *ram* e a outros meios de armazenamento, ativar a *webcam* e gerar coordenadas de localização do computador. O único objetivo era obter informações tais como: registos dos endereços IP utilizados; registos da atividade na *internet*, incluindo *logs*, *caches*, *browser*, histórico, *cookies*, páginas marcadas como favoritas, termos de pesquisa e sites pesquisados; registos que comprovassem a utilização daquele endereço IP para aceder ao *e-mail* de John Doe; provas como no momento dos factos descritos o 'atacante' usou, apropriou ou controlou o computador de John Doe a fim de criar, editar ou apagar, nomeadamente, provas como *logins*, usuários e palavras-passe, documentos, histórico de navegação, perfis, conteúdos e contactos de *e-mails*, *chat*, entre outros; provas que o *software* utilizado permitia que terceiros pudessem também controlar o computador da vítima e prova do número de vezes que o mesmo foi acedido.

Em suma, o FBI, no decorrer da investigação, perspetivava obter os seguintes dados: (1) registos de entradas que pudessem identificar novas fraudes; (2) fotografias tiradas pela *webcam* do computador infetado, de forma a identificar a sua localização e as pessoas que o utilizavam; (3) informações sobre a localização física do computador infetado, incluindo as suas coordenadas; e (4) registos das aplicações em curso.

O aludido pedido foi feito ao abrigo do regime aplicável às buscas e apreensões do artigo 41.º do *Federal Rules of Criminal Procedure*[88], que assentou no enquadramento, por um lado, da instalação de *malware* no conceito de busca e, por outro, da extração e envio de informações remotas no conceito de apreensão.

O tribunal analisou este pedido, com base nas seguintes questões: (1) competência territorial; (2) requisitos específicos da quarta Adenda à Constituição dos Estados Unidos da América; e (3) requisitos da quarta Adenda relativos à videovigilância.

3.1.2.1 Competência territorial

No que diz respeito à competência territorial, a letra b do artigo 41.º estabelecia um conjunto de cinco[89] situações quanto aos limites territoriais em que era possível a aplicação do mandado. Todavia, o pedido do FBI não se enquadrava em nenhum desses casos, conforme veremos[90].

Por um lado, o FBI reconheceu, desde logo, que era ignorada a localização física do sistema informático, mas justificou a possibilidade de requerer o mandado considerando que a informação recolhida iria ser examinada dentro do âmbito territorial

---

[88] Para melhor acompanhar este artigo, poderá consultar o *Federal Rules of Criminal Procedure*, disponível em http://www.uscourts.gov/rules-policies/current-rules-practice-procedure [consultado a 16-10-2016]. Saliente-se que o artigo 41.º foi alterado em dezembro de 2016, permitindo desde essa data a emissão de mandado, quando a localização do sistema é desconhecida, mas sempre mediante a verificação de determinados pressupostos. Cf. MIRJA GUTHEIL *et al.*, *Legal Frameworks for*…, op. cit., p. 122.

[89] *Rule 41. Search and Seizure (b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government: (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district; (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed; (3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district; (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following: (A) a United States territory, possession, or commonwealth; (B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.*

[90] Para uma descrição mais detalhada dos argumentos utilizados pelo tribunal, quanto a esta questão, consultar a decisão disponível em https://www.gpo.gov/fdsys/pkg/USCOURTS-txsd-4_13-mj-00234/pdf/USCOURTS-txsd-4_13-mj-00234-0.pdf [consultada a 11-10-2016].

do distrito de Houston, Texas. O tribunal não acompanhou esta interpretação, porque a mesma permitiria ao órgão que investiga 'percorrer o mundo' em busca de provas, desde que as mesmas só fossem acedidas no distrito onde foi emitido o mandado.

Por outro, o pedido do FBI assentava numa dupla perspetiva: (1) a busca ao computador em si; e (2) a busca aos dados informáticos no/e gerados pelo computador. O tribunal concluiu, ao contrário da analogia que era feita pelos fornecedores de serviço de *internet*, que a informação digital não se encontrava armazenada em 'nuvem', mas num sistema informático que só por si tinha uma localização física, logo, estava sujeita às regras jurisdicionais do Estado onde se encontrava. Assim, antes dos dados poderem ser acedidos pelo FBI num computador localizado no distrito de Houston/Texas, teria de se realizar uma busca no computador visado e essa busca não tinha lugar no ciberespaço, mas sim num lugar físico, associado a uma morada e a um proprietário.

Em suma, como a localização do sistema visado era desconhecida e, em consequência, os dados informáticos também o eram, concluiu o tribunal que não estavam preenchidos os limites territoriais da letra b) do n.º 1 do artigo 41.º [91].

3.1.2.2 Requisitos específicos da quarta Adenda

Relativamente aos requisitos específicos da quarta Adenda à Constituição Norte-Americana, a mesma previa que nenhum mandado de busca e apreensão deveria ser emitido sem que houvesse um motivo razoável e uma causa provável. O mesmo teria de discriminar o lugar onde se efetuaria a busca, os objetos a serem apreendidos e os sujeitos que seriam alvo da técnica.

No caso em apreciação, o mandado tinha como objetivo duas buscas diferentes: (1) ao computador visado como instrumento da infração; e (2) ao computador como prova da atividade criminosa.

Entendeu o tribunal que o pedido do FBI pouco ou nada referia, quanto à forma como o sistema informático do suspeito seria acedido, apenas invocando que o método pelo qual o *software* seria introduzido se encontrava concebido para garantir que o visado seria o único indivíduo lesado. Subentendeu o tribunal que o FBI iria entrar em

[91] Note-se que o tribunal continuou a analisar o pedido do FBI, com base nas restantes subseções do artigo 41.º. Como consideramos que esta análise não se revela interessante para o presente estudo, não a desenvolvemos aqui. Quanto a uma análise mais detalhada dos argumentos utilizados, consultar https://www.gpo.gov/fdsys/pkg/USCOURTS-txsd-4_13-mj-00234/pdf/USCOURTS-txsd-4_13-mj-00234-0.pdf. [consultada a 11-10-2016].

contacto com o computador do visado, através de um *e-mail* falso, no pressuposto de que apenas este teria acesso aquela conta de *e-mail*.

Partindo dessa suposição, entendeu o tribunal que o procedimento não oferecia garantias de que só aquele sistema informático seria acedido, até porque não raras as vezes os sujeitos envolvidos em atividades criminosas falsificam os endereços IP, como forma de ocultar a sua presença no mundo *online*, razão pela qual a busca do FBI poderia ser dirigida a um ou mais sistemas inocentes no percurso até ao computador visado.

Face ao exposto, o tribunal indeferiu o pedido do FBI, alegando para o efeito que o mesmo não apresentava garantias de que a técnica utilizada evitaria infetar sistemas inocentes, nem detalhava o método que seria utilizado. Levantou, ainda, as seguintes questões: "*E se o computador visado estiver localizado numa biblioteca pública, ou num café com internet, ou num local de trabalho acessível a outros? E se o computador for usado pela família ou amigos não envolvidos no esquema criminoso? E se o e-mail falso for usado para fins legítimos por outros indivíduos não relacionados com a atividade criminosa? E se o e-mail for acedido por mais do que um computador, ou por um telemóvel ou outro dispositivo informático?*[92].

Por fim, e embora o tribunal tivesse entendido que o pedido do FBI não respeitava os requisitos da quarta Adenda à Constituição, designadamente quanto à busca no sistema informático visado, alertou que pedidos semelhantes podiam ser deferidos na condição de apontarem respostas às questões que ora tinham sido levantadas.

3.1.2.3 Requisitos da quarta Adenda relativos à videovigilância

Como referido anteriormente, o *software* que o FBI pretendia instalar permitia ativar a *webcam* do computador infetado e tirar fotografias das pessoas que o utilizavam. O FBI descreveu esta técnica como "*photo monitoring*" em oposição à videovigilância. Todavia, o tribunal considerou que esta distinção era indiferente, porque ao tirarem-se fotografias também se teria acesso em tempo real à *webcam*, motivo pelo qual o referido acesso equivaleria a uma atividade de videovigilância.

Um pedido para autorização de videovigilância deveria demonstrar não só que a prova seria capturada através deste meio, mas inclusive deveria conter o seguinte: (1)

[92] Tradução nossa.

justificação como outros meios de investigação foram utilizados e não obtiveram sucesso ou, que de outra forma seria impossível recolher prova; (2) uma descrição detalhada do tipo de comunicações que se procurariam intercetar e qual o crime em causa; (3) duração do meio, tendo em atenção que a mesma não poderia ser superior ao estritamente necessário para o fim a que se destinava[93]; e (4) medidas a tomar para garantir que o método seria o menos lesivo possível para prosseguir os seus fins.

Neste caso, o pedido do FBI apenas mencionava que existiam razões para considerar que outros meios para aceder à *webcam* se revelariam infrutíferos, mas não oferecia garantias suficientes de que terceiros não seriam lesados. Limitou-se, para o efeito, a referir que seriam tomadas medidas de forma a garantir que o método prosseguiria apenas os fins do mandado, até porque o *software* não tinha sido concebido para procurar, capturar, revelar ou distribuir informações ou uma ampla gama de dados, mas sim para capturar uma quantidade limitada de informações minimamente necessárias para identificar a localização do computador visado e o seu utilizador.

Não obstante, entendeu o tribunal, por um lado, que as medidas que seriam tomadas para recolher os dados estritamente necessários não foram especificadas. Por outro, que um *software* que tinha sido concebido para capturar apenas uma quantidade limitada de dados não mitigaria o risco de uma busca mais abrangente, sendo essa garantia fatalmente indeterminada pela amplitude de dados que o *software* podia recolher. Dito por outras palavras, concluiu o tribunal que um *software* que era capaz de recolher um volume tão grande de informações como histórico da *internet*, termos de pesquisa, conteúdo dos *e-mails* e contactos, *chat*, fotografias, correspondência, aplicações em curso, entre outros, não poderia simplesmente ser descrito pelo FBI como "*apenas capaz de capturar uma quantidade limitada de dados*".

Por todas estas razões, entendeu o tribunal que o pedido de mandado não estava suficientemente fundamentado, e não existia informação bastante para concluir com segurança que o *malware* não seria instalado noutros sistemas, persistindo a possibilidade da *webcam* transmitir imagens de pessoas não envolvidas na atividade criminosa. Em consequência, no que diz respeito à videovigilância, não se encontravam preenchidos os requisitos da quarta Adenda à Constituição.

[93] Neste caso, não podia ser superior a trinta dias, prorrogável por igual período.

Todavia, o tribunal adiantou que a utilização de um meio oculto semelhante pode ser requerida nos termos do artigo 41.º, pois poderão existir razões para atualizar[94] os requisitos da competência territorial à luz dos avanços tecnológicos, contudo, deverá sempre haver uma cuidadosa adesão às restrições do artigo, sem deixar de mencionar obrigatoriamente a quarta Adenda.

Em síntese, o pedido de busca e apreensão foi indeferido[95] nestes termos: não oferecia garantias de que só o mínimo necessário de dados seria recolhido; não assegurava que apenas o visado seria alvo deste meio e que terceiras pessoas não iriam instalar, involuntariamente, o *malware* no seu sistema informático; e não estavam verificados os pressupostos da indispensabilidade e limites para o recurso à videovigilância.

3.1.3 Operação Torpedo

Em agosto de 2011, a *National High Tech Crime Unit* (NHTCU) da Holanda iniciou uma grande operação de combate à pornografia infantil na rede *Tor*[96]. Ativou um rastreador *web*[97] que percorreu a *dark web* e, consequentemente, permitiu a recolha de vários endereços *Tor Onion*.

O *Tor*, também conhecido por *Tor Onion Router*, foi originalmente desenhado, implementado e desenvolvido pelo projeto da *U.S Naval Research Laboratory* com o intuito de proteger as comunicações governamentais e está atualmente disponível na *internet* para *download*.

O *software Tor* protege a privacidade dos seus utilizadores, reenviando, aleatoriamente, as comunicações através de uma série de retransmissores[98] que visam tornar anónima e não identificável a origem e o destinatário das mesmas. Assim, permite mascarar, em camadas, o endereço IP real do utilizador que, de outro modo,

---

[94] Como se referiu na nota 88, os requisitos já foram revistos.
[95] Decisão disponível em https://www.gpo.gov/fdsys/pkg/USCOURTS-txsd-4_13-mj-00234/pdf/USCOURTS-txsd-4_13-mj-00234-0.pdf e http://md.fd.org/cja2014/nov2014/riley/In_re_warrant_to_search_a_target_computer_at_premises_unknown.pdf [consultadas a 11-10-2016].
[96] Cf. KEVIN POULSEN, «Visit the Wrong Website and the FBI Could End Up in Your Computer», *WIRED*, 05-08-2014, disponível em https://www.wired.com/2014/08/operation_torpedo/ [consultado a 09-10-2016].
[97] Um rastreador *web* é um *software* que pode ser utilizado para pesquisar automaticamente *sites* e identificar hiperligações disponíveis nos mesmos.
[98] Isto é, em torno de uma rede de computadores distribuída entre vários voluntários de todo o mundo.

poderia ser identificado, tornando praticamente impossível traçar a comunicação até ao IP real.

O *Tor* também permite a criação de *websites* designados por *hidden services* que operam na rede de modo a que fique escondido o endereço IP dos servidores nos quais se encontram alojados. Os *hidden services* funcionam da mesma forma que os vulgares *websites* com a diferença de que os primeiros assumem a forma de identificação de endereços complexos gerados por um algoritmo terminado em "*.onion"*. Apenas os utilizadores do *Tor*, que operam na sua rede, conseguem aceder a estes *hidden services.*

Os agentes holandeses visitaram cada um dos *hidden services* que recolheram e, posteriormente, elaboraram uma lista daqueles que indiciavam dedicar-se à pornografia infantil. Posto isto, solicitaram um mandado ao tribunal de Roterdão, nomeadamente, para identificar a localização física dos seus servidores.

A 15 de agosto de 2011, a NHTCU identificou um *hidden service*, designado por "Hidden Service B" (mas com o nome real de "Pedoboard"), que continha numerosas imagens de pornografia infantil. Ao aceder ao mesmo, verificou que o administrador não tinha sido devidamente cauteloso, pois não possuía uma palavra-passe na sua conta, permitindo que a NHTCU fizesse *login* e tivesse completo acesso ao *hidden service*.

Não obstante, devido à natureza anónima do *Tor*, há forte probabilidade de a presença dos agentes vir a ser descoberta pelo administrador, e perante a possibilidade e o receio de que as provas fossem eliminadas, os agentes copiaram previamente todo o conteúdo deste *hidden service* para um servidor localizado na Holanda. Só após esta etapa, é que ganharam o acesso e o controlo do mesmo.

Nessa altura, descobriram a existência de vários endereços IP's associados ao *hidden service*, nomeadamente, os endereços 70.34.32.235, 70.34.32.112, 74.34.32.1 e 70.34.32.3. Em consequência, fizeram um pedido para a apresentação de dados que demonstrou que aqueles endereços se encontravam nos Estados Unidos da América.

Os agentes também encontraram na configuração da rede *Tor* um arquivo que revelou naquele servidor a existência de outros dois *hidden services*: o "Hidden Service C", cujo nome real estava associado a menores; e o "Hidden Service D" que continha imagens de menores. Porém, foi num exame mais profundo que acabaram por detetar a presença de um terceiro *hidden service*: o "Bulletin Board A", o qual continha pornografia infantil.

Em síntese, o "Bulletin Board A"[99], no mês de dezembro de 2012, tinha mais de 5600 membros, 3000 tópicos de mensagens e 24000 publicações. O mesmo encontrava-se organizado em três categorias: "board"; "imagens"; e "texto".

Dentro do fórum "board" existiam três sub-fóruns: "informações"; "questões"; e "comentários". Por sua vez, o fórum "imagens" estava organizado em fotografias de "bebés", "meninos ou meninas na pré-adolescência" e "meninos ou meninas adolescentes". Por fim, o fórum "texto" englobava cinco sub-fóruns: "pedo talk"; "links"; "freenet"; e "histórias". Nestes fóruns, os temas abordados iam desde questões relacionadas com o abuso sexual de crianças, nomeadamente, métodos e táticas para perpetrar o abuso, a conselhos de segurança e/ou anonimato ou *modus operando* em caso de investigação[100].

Durante os meses em que os agentes do FBI monitorizaram a atividade do "Bulletin Board A", observaram diversas publicações e respostas a questões no "pedo talk". Citam-se alguns exemplos que, pelo seu carácter, consideramos perturbantes: "*Como encontrar uma criança que possa aliciar a fazer-me favores sexuais*"; "*Qual a melhor idade para isto*?"; *Como atrair uma criança até ao meu carro?*"; "*Arranja um emprego de baby-sitter*"; e "*Se precisares envia-me uma mensagem privada, posso ajudar nisso*"[101]. Os agentes também verificaram publicações de fotografias de bebés, crianças ou pré-adolescentes nus ou envolvidos em atos de cariz sexual com adultos ou outras crianças.

3.1.3.1 O *Bulletin Board A*

Era extremamente improvável que alguém chegasse até ao "Bulletin Board A", sem saber que género de *website* se tratava, isto é, não se podia dar o caso de alguém ser 'apanhado' a visitar um *website* destes por um mero acaso ou engano. Os utilizadores do "Bulletin Board A" só tinham conhecimento do endereço *web* através de outros *users* ou por *posts* na *internet* que falassem do tipo de conteúdo ali disponível.

---

[99] O URL deste *hidden service* era: http://jkpos24pl2r3urlw.onion.

[100] Um dos conselhos era a utilização do TrueCrypt, o qual deixou de estar disponível em maio de 2014. Era uma aplicação *open source* para o *Windows*, *Mac* e *Linux* que permitia a criação de volumes encriptados e montados como unidades virtuais. Em suma, tinha a capacidade de criar discos virtuais encriptados como se de um disco real se tratasse. Cf. https://informaticaemportugues.wordpress.com/2013/03/19/truecrypt-funcionalidades/ [consultado a 20-11-2016].

[101] Tradução nossa.

À semelhança do que já havia feito com o “Hidden Service B”, a NHTCU copiou também previamente todo o conteúdo do “Bulletin Board A", recorrendo a diversos programas de *software*. Posto isto, ganhou acesso ao servidor que o hospedava, verificando que o endereço IP era o 98.161.25.30.

Através de um pedido para a apresentação de dados, os agentes descobriram que este IP, à semelhança dos outros, também se encontrava nos Estados Unidos da América, pertencendo ao prestador de serviços *Cox Communications* que, por sua vez, estava atribuído ao serviço de *internet* da cliente Tiffany Strasser, com a morada 510 Piedmont Dr., Omaha, NE 68154.

Face à localização dos endereços IP, a NHTCU solicitou a colaboração do FBI. Os agentes do FBI descobriram que os servidores pertenciam à empresa *PowerDNN*, sedeada em Bellevue, Nebraska, a qual se dedicava ao fornecimento de serviços de hospedagem.

Após um pedido para apresentação de dados, o FBI certificou-se de que os referidos servidores não estavam a ser utilizados por nenhum cliente da aludida empresa, concluindo que os *hidden services* neles hospedados deveriam pertencer a alguém com acesso aos mesmos, por exemplo, um trabalhador.

Com as informações prestadas pelo fornecedor de serviço *Cox Communications*, o FBI solicitou ao *United States Postal Service* que indicasse quem residia naquele endereço, acabando por concluir que apenas lá residiam Tiffany Strasser e Aaron McGrath.

O FBI vigiou a atividade de Aaron McGrath, durante um período de trinta dias, ao fim do qual concluiu que a rede *wi-fi* da sua residência era aberta ao público, ou seja, não possuía uma palavra-passe. Também verificou no perfil do *Facebook* (que não tinha restrições de privacidade) que o mesmo trabalhava na *Perigon Networks*, e que esta funcionava no mesmo edifício que a *PowerDNN* (1001 N Fort Crook Rd., Suite 145, Bellevue, Nebraska 68005).

Uma breve pesquisa ao *website* das empresas permitiu averiguar que estas foram criadas e fundadas pela mesma pessoa, tendo a mesma sede. Verificaram, também, que Aaron McGrath prestava apoio aos servidores da *PowerDNN*.

Posteriormente, o FBI solicitou um pedido para apresentação de dados ao *Facebook*, tendo o mesmo informado que a perfil de McGrath estava associado ao endereço de *e-mail* wytecastl@gmail.com. Tal facto levou o FBI a solicitar ao *Google* a prestação de informações, tendo-lhe sido comunicado que aquele *e-mail* pertencia ao

utilizador Aaron McGrath e estava associado ao *e-mail* alternativo mcgrath@powerdnn.com. O FBI concluiu, assim, que existia uma grande probabilidade de McGrath ter acesso aos servidores onde os *hidden services* estavam hospedados.

A 29 de agosto de 2011, o *United States Department of Justice* emitiu um pedido de colaboração às autoridades competentes holandesas, ao abrigo do *U.S – Netherlands Mutual Legal Assistance Agreement*, respetivo anexo, e da Convenção sobre o Cibercrime, solicitando o acesso às provas recolhidas e apreendidas pela NHTCU no âmbito da sua investigação.

Em outubro de 2011, o FBI teve acesso ao disco rígido que continha as provas apreendidas dos mencionados servidores e, coadjuvado por especialistas em computação forense, analisou o conteúdo do mesmo.

Durante um ano, o FBI vigiou a atividade de McGrath enquanto, paralelamente, trabalhava na ferramenta legal que se tornaria na "Operação Torpedo"[102].

Em abril de 2012, depois de uma interceção para a recolha de dados da *internet*, o FBI teve a confirmação de que um dos utilizadores daquele serviço, isto é, a Tiffany ou o Aaron, acedia frequentemente à rede *Tor* e também aos servidores localizados na *PowerDNN*, com os endereços IP 208.88.72.99, 208.88.75.208, 208.88.77.241, 208.88.77.244, 208.88.78.230, 208.88.78.30, 208.88.78.40 e 70.34.34.106.

A maioria das conexões com a *internet* e os servidores da *PowerDNN* envolvia o servidor com o endereço IP 208.88.77.241 e, entre 1 a 24 de outubro de 2012, a conta de *internet* estava conectada a, pelo menos, catorze diferentes IP's atribuídos à *PowerDNN*, sendo novamente o servidor com o endereço IP 208.88.77.241 o mais visitado.

Uma consulta de dados publicamente disponíveis permitiu verificar que os servidores acedidos a partir da casa de Strasser e McGrath não hospedavam qualquer *website* publicamente acessível. Dos dados recolhidos pela interceção resultou que o "Bulletin Board A" provavelmente estaria hospedado num dos servidores da *PowerDNN*, mas era acedido a partir de casa do suspeito.

Esta teoria foi corroborada, em agosto de 2011, com a publicação do administrador do "Bulletin Board A" da informação de que o mesmo seria encerrado por algum tempo (o que coincide com o acesso da NHTCU) e, posteriormente, com a publicação, em 13 de outubro de 2011, informando que *hidden service* já estava

[102] Cf. KEVIN POULSEN, «Visit the Wrong Website…», op. cit.

disponível e que tinham procedido à transferência do mesmo para um sistema de hospedagem diferente.

A 15 de novembro de 2012, o FBI confirmou junto de Tony Valenti, proprietário e fundador da *PowerDNN* e da *Perigon Networks*, que todos os endereços IP iniciados por "208" se localizavam em Cosentry, 1001 N. Fort Crook Road, Suite 132, incluindo o endereço IP 208.88.77.241. Perante isto, o referido servidor foi apreendido e transferido para as instalações do FBI, onde continuou a funcionar.

Na mesma data, os agentes fizeram uma busca a casa de Aaron McGrath, encontrando o mesmo no computador portátil, que rapidamente fechou, bloqueando-o. Após terem conseguido desbloquear o computador, os agentes encontraram aberto um separador de *internet* onde Aaron estava conectado ao "Bulletin Board A" como administrador, através do endereço IP 208.88.77.241.

Verificou-se que Aaron McGrath, entre janeiro de 2009 e novembro de 2012, tinha criado e administrava os três *hidden services* dedicados à produção e distribuição de pornografia infantil[103].

3.1.3.2 Pedido para utilização de *malware* no "*Bulletin Board A*"

Além do mandado de busca a casa de Aaron McGrath, foram solicitados três mandados separados, um para cada *hidden service*[104].

Os referidos mandados permitiam ao FBI modificar o código dos servidores e, consequentemente, propagar uma NIT (*Network Investigative Technique*)[105] em cada computador que acedia àqueles *websites*.

No que diz respeito ao "Bulletin Board A", a 15 de novembro de 2012, o agente do FBI, Jeffrey Torpinian, solicitou ao tribunal do distrito de Nebraska um mandado[106] para aceder a este *hidden service*. Na base do pedido estava o facto do "Bulletin Board A" funcionar na rede *Tor*, permitindo, em consequência, aos seus utilizadores mascarar o endereço IP real, o que tornava impossível rastrear as comunicações, razão pela qual as outras técnicas tradicionais revelar-se-iam infrutíferas na obtenção de prova, não restando outra alternativa que a de recorrer ao uso da NIT.

---

[103] Cf. memorando disponível em http://www.leagle.com/decision/In%20FDCO%2020140203910.xml/U.S.%20v.%20McGRATH [consultado a 01-11-2016].
[104] Cf. KEVIN POULSEN, «Visit the Wrong Website…», op. cit.
[105] A qual, por outras palavras, significa *malware*.
[106] Este requerimento está disponível para consulta em https://www.documentcloud.org/documents/1261620-torpedo-affidavit.html [consultado a 22-10-2016].

Através da NIT, os agentes do FBI, durante o período de trinta dias, procurariam investigar qualquer usuário que acedesse ao fórum "imagens", assim como aqueles que enviavam e liam mensagens privadas no "Bulletin Board A".

A NIT foi concebida para enviar secretamente um determinado conteúdo malicioso a cada visitante/utilizador que acedesse aos supracitados locais e, consequente e automaticamente, obrigava o seu sistema informático a fazer *download* desse conteúdo.

Instalada a NIT no sistema informático dos suspeitos, esta enviaria secretamente dados para um servidor do FBI, sem que o seu utilizador se apercebesse desta situação, porque a NIT não comprometia as funções da máquina.

As informações enviadas visavam identificar a localização do sistema informático e o seu utilizador[107], através de: (1) endereço IP real do computador, bem como a data e a hora em que este foi reconhecido; (2) identificação da sessão ativa; e (3) tipo de sistema operacional em execução, nomeadamente, a versão e arquitetura (por exemplo *Windows* 7, X86).

Posteriormente, os dados recolhidos iriam permitir ao FBI associar: (1) o endereço IP real do sistema que acedia ao "Bulletin Board A" a um determinado provedor de serviços de *internet* para, em consequência, identificar o cliente; (2) a sessão aberta e o seu real utilizador, excluindo os restantes que poderiam utilizar também aquele sistema; e (3) numa busca, o sistema operacional a um determinado sistema informático de entre os restantes provavelmente existentes no local.

Neste pedido, também foi solicitado pelo agente do FBI que o mandado fosse secreto, isto é, sem prévio aviso da sua utilização. Justificou o seu pedido no facto de uma notificação imediata (ainda que os suspeitos a notificar fossem desconhecidos) poder frustrar a investigação, nomeadamente, porque os utilizadores deixariam de aceder ao "Bulletin Board A" ou tomariam outros meios de ocultação.

Em duas semanas, o FBI recolheu o endereço IP real de pelo menos vinte e cinco visitantes daquele *hidden service*[108] e, através da apresentação de dados dos provedores de serviços, identificou os suspeitos e as suas moradas.

Cinco meses após a instalação da NIT, foram feitas buscas e detenções por todo o país. Dos vinte e cinco visitantes, dezanove foram conduzidos até julgamento, entre 2014 e 2015. Durante todo o processo, foi posta em causa a utilização de *malware*,

[107] Pese embora existirem rumores de que também era um *malware* do tipo *keylogger*.
[108] Cf. KEVIN POULSEN, «Visit the Wrong Website…», op. cit.

alegando a defesa a nulidade da prova, visto que não foi respeitado o período de duração do meio, havendo arguidos que tiveram conhecimento do recurso a NIT, só um ano depois da operação.

Não obstante, a verdade é que devido à utilização de *malware* foi possível condenar dezanove dos indivíduos: Jason Flanary[109]; Timothy Deffogi[110]; Zackary Austin[111]; Russel Glenn Pierce[112]; David William Peer; Joshua Welch[113]; Thomas Spencer[114]; Michael Huyck[115]; Brandon Moore; John Sebes[116]; Gary Reibert; Kirk Cottom; Kevin M. Pitman; Vicent Diberardino; Wesley Cameron; Charles MacMillan; Warren Tidwell; David Smith[117] e Aaron McGrath[118].

---

[109] Para mais informações sobre este processo consultar https://www.gpo.gov/fdsys/search/pagedetails.action?na=&se=&sm=&flr=&ercode=&dateBrowse=&govAuthBrowse=&collection=&historical=false&st=Jason+Flanary&psh=&sbh=&tfh=&originalSearch=&fromState=&sb=re&sb=re&ps=10&ps=10&granuleId=USCOURTS-ned-8_13-cr-00104-1&packageId=USCOURTS-ned-8_13-cr-00104 [consultado a 20-11-2016].

[110] Para mais informações sobre este processo consultar https://www.gpo.gov/fdsys/search/pagedetails.action?st=Timothy+Defoggi&granuleId=USCOURTS-ned-8_13-cr-00105-29&packageId=USCOURTS-ned-8_13-cr-00105&fromState [consultado a 20-11-2016].

[111] Cf. sentença disponível em https://www.gpo.gov/fdsys/pkg/USCOURTS-ned-8_13-cr-00105/pdf/USCOURTS-ned-8_13-cr-00105-24.pdf [consultada a 20-11-2016].

[112] Cf. Sentença disponível em https://www.gpo.gov/fdsys/pkg/USCOURTS-ned-8_13-cr-00106/pdf/USCOURTS-ned-8_13-cr-00106-38.pdf [consultada a 20-11-2016].

[113] Cf. sentença disponível em https://www.gpo.gov/fdsys/pkg/USCOURTS-ned-8_13-cr-00106/pdf/USCOURTS-ned-8_13-cr-00106-32.pdf [consultada a 20-11-2016].
Cf. recurso disponível em https://www.gpo.gov/fdsys/pkg/USCOURTS-ca8-15-01993/pdf/USCOURTS-ca8-15-01993-0.pdf [consultado a 20-11-2016].

[114] Cf. sentença disponível em https://www.gpo.gov/fdsys/pkg/USCOURTS-ned-8_13-cr-00106/pdf/USCOURTS-ned-8_13-cr-00106-34.pdf [consultada a 20-11-2016].

[115] Para mais informações sobre este processo consultar https://www.gpo.gov/fdsys/search/pagedetails.action?na=&se=&sm=&flr=&ercode=&dateBrowse=&govAuthBrowse=&collection=&historical=false&st=Michael+Huyck&psh=&sbh=&tfh=&originalSearch=&fromState=&sb=re&sb=re&ps=10&ps=10&granuleId=USCOURTS-ned-8_15-cr-00044-5&packageId=USCOURTS-ned-8_15-cr-00044 [consultado a 20-11-2016].

[116] Cf. sentença disponível em https://www.gpo.gov/fdsys/pkg/USCOURTS-ned-8_13-cr-00107/pdf/USCOURTS-ned-8_13-cr-00107-35.pdf [consultada a 20-11-2016].

[117] Cf. sentença disponível em https://www.gpo.gov/fdsys/pkg/USCOURTS-ned-8_13-cr-00108/pdf/USCOURTS-ned-8_13-cr-00108-21.pdf [consultada a 20-11-2016].

[118] Cf. informação disponível em https://www.gpo.gov/fdsys/pkg/USCOURTS-ned-8_12-cr-00422/pdf/USCOURTS-ned-8_12-cr-00422-7.pdf [consultado a 20-11-2016].
Cf. sentença disponível em http://www.morelaw.com/verdicts/case.asp?n=8:13-cr-00108-JFB-TDT&s=NE&d=86431 [consultada a 24-11-2016].

Da análise dos casos acima referidos facilmente se conclui que o *malware* como meio oculto pode ter inúmeras características. Em termos genéricos, pode recolher todo o tipo de dados, intercetar comunicações e vigiar em tempo real os arguidos ou suspeitos.

Assim, este meio encoberto deve ser concebido e estruturado apenas com determinadas características, dito de outro modo, não deverá existir um *software* malicioso único que englobe em si todas as potencialidades permitidas, mas antes deverá ser criado, em cada caso, um *malware* adequado ao fim pretendido. Só assim será possível ao juiz controlar o grau de lesão que o mesmo terá.

Em consequência, o requerimento e o despacho que autorize este meio encoberto deverão ser bastante detalhados, nomeadamente: têm de demonstrar o motivo razoável e a causa provável para o recurso a este meio; discriminar, caso seja possível, o sistema informático e as unidades de armazenamento a aceder; o lugar onde se encontra o sistema (sempre que haja essa informação); os dados que se pretendem ou se poderão recolher; o género de comunicações a intercetar; os sujeitos em causa; a forma como se pretende aceder ao sistema informático; o prazo de duração; e meio de garantir a cadeia de custódia.

No fim da operação, é essencial e imperativo a elaboração de um relatório detalhado, onde se discrimine o procedimento, isto é, as medidas adotadas para garantir que aquele sistema é o único infetado, os dados recolhidos e as medidas tomadas na sua recolha.

Por último, como vimos, no recurso a este meio poderá ser importante a cooperação judiciária entre países, quando o sistema informático ou os dados estão fora do seu âmbito da competência territorial. O já aludido estudo do Parlamento Europeu aponta esta questão como uma das que devem ser estudadas e desenvolvidas pelos Estados Membros, propondo uma aproximação de leis, introdução de normas mínimas e técnicas de investigação comuns, de forma a facilitar o reconhecimento mútuo de elementos de prova, decisões judiciais, entre outros[119].

3.2 A política legislativa na Europa

No presente capítulo pretende-se fazer uma análise de seis regimes jurídicos europeus que prevêem o uso de *malware*, de molde a termos uma visão geral dos

[119] Cf. MIRJA GUTHEIL *et al*., *Legal Frameworks for*…, op. cit., pp. 34-36.

pressupostos para a utilização deste meio encoberto. Mais especificamente, pretendemos observar o juízo de ponderação efetuado em cada um dos casos, a fim de assegurar a legalidade, necessidade e proporcionalidade deste método oculto face à restrição dos direitos fundamentais. O nosso objetivo é, no capítulo final, apresentarmos os requisitos e pressupostos necessários para a autorização do uso de *malware*.

O critério de escolha dos países fundou-se, essencialmente, na proximidade geográfica, jurídica e maturidade legislativa. Optámos por analisar a política legislativa, adotada e em vigor na Alemanha, Espanha, Estónia, Finlândia e França, respetivamente desde 2008, 2015, 2013, 2014 e 2011, e ainda o Projeto de Lei Quintarelli (Itália), apresentado em fevereiro de 2017.

3.2.1 Alemanha

A 20 de dezembro de 2006, foi introduzido na Lei de Proteção da Constituição da Renânia do Norte-Vestefália[120] o § 5.2 (11)[121] que admitia o recurso ao *malware*. Contudo, o Tribunal Constitucional Federal Alemão acabou por concluir que o § 5.2 (11) violava os princípios da proporcionalidade, da clareza e certeza legal, pelo que se pronunciou pela sua inconstitucionalidade[122].

A 25 de dezembro de 2008, com base nos requisitos que o Acórdão do Tribunal Constitucional indicou, a Lei para a Defesa Face aos Perigos do Terrorismo Internacional (*Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt*)[123] introduziu no ordenamento jurídico alemão (reformando a *Bundeskriminalamtgesetz* [*BKA-Gesetz*]) a possibilidade de recurso ao *malware*. Esta reforma teve como intuito regular importantes e avançados meios de investigação criminal.

Ora, o § 20k da Lei para a Defesa Face aos Perigos do Terrorismo Internacional[124], sob a epígrafe vigilância secreta em sistemas de informação, permite à polícia federal, sem o conhecimento da pessoa visada, aceder ao seu sistema informático, com o intuito de recolher dados.

---

[120] Esta lei descreve os direitos e estabelece uma base legal para as operações da Agência de Proteção da Constituição, que é o principal serviço secreto alemão para os assuntos internos.
[121] O artigo define quais as ações admissíveis para obtenção de informações e dados privados dos suspeitos.
[122] Cf. JUAN CARLOS ORTIZ PRADILLO, «El *Remote Forensic*…», op. cit., pp. 4-6.
[123] Cf. *Ibidem*, pp. 5-6.
[124] Poderá consultar a mesma em http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl108s3083.pdf [consultada a 05-12-2016].

Este meio é permitido nos casos em que se verifique perigo para a vida, para a integridade física ou para a liberdade de determinada pessoa e para a liberdade ou segurança nacional, assim como, em casos de prevenção de terrorismo a nível internacional ou relacionados com as infrações previstas no § 129a do StGB (§ 4a). Mas, apenas se for muito difícil ou impossível alcançar o mesmo resultado, através de outro meio de obtenção de prova menos gravoso.

No que se refere à competência, o recurso ao *malware* só poderá ser autorizado pelo presidente do Tribunal Federal ou por seu representante. O despacho de autorização deverá: (1) indicar a pessoa que será atingida, se possível, identificando-a com o nome e morada; (2) descrever, o mais detalhadamente possível, o sistema informático onde serão recolhidos os dados; (3) indicar a natureza e a duração do meio; e (4) fundamentar o uso de *malware*. Não obstante, o recurso a este meio não será autorizado, se houver indícios concretos de que serão recolhidos apenas dados referentes à vida privada do indivíduo ou se for impossível garantir que a técnica utilizada não irá recolher esse tipo de dados.

Os dados recolhidos, nos termos do § 5, serão automaticamente remetidos para análise da Comissão de Proteção de Dados e de dois funcionários federais, podendo um deles ser o juiz. Esta análise tem como objetivo a verificação do conteúdo dos dados recolhidos, designadamente se dizem respeito ao núcleo central da vida privada ou não. Em caso afirmativo, serão imediatamente eliminados, sendo elaborado um relatório para efeitos de controlo e proteção de dados. O mesmo será destruído quando deixar de ser necessário ao aludido fim, sempre com o limite máximo de um ano civil, a contar da data da sua elaboração[125]. Os restantes dados serão guardados até ao final do ano civil seguinte ao da investigação, sendo posteriormente eliminados[126].

Relativamente ao catálogo de sujeitos, determina esta norma que só poderão ser visados os suspeitos nos termos do §17 e §18 da Lei da Policia Federal (*Bundespolizeigesetz*).

No que se refere ao prazo, este meio terá a duração máxima de três meses, renovável por igual período, desde que se verifiquem os respetivos requisitos de

[125] Determinou o Tribunal Constitucional Federal Alemão que este procedimento era insuficiente para garantir a proteção da área central da vida privada. Os dados devem ser examinados por uma entidade independente. Cf. BVerfG, Judgment of the First Senate of 20 April 2016 - 1 BvR 966/09, disponível em http://www.bverfg.de/e/rs20160420_1bvr096609en.html [consultado a 01-05-2017].

[126] O Tribunal Constitucional Federal Alemão considerou esta parte inconstitucional, uma vez que é um prazo demasiado curto para serem analisados, antes de serem eliminados. Cf. *Ibidem*.

admissibilidade. Se estes deixarem de se verificar, a investigação será imediatamente interrompida.

Quanto ao procedimento, só são admitidas técnicas que realizem o mínimo de alterações no sistema informático e que permitam a sua reversão. As técnicas utilizadas devem proteger o sistema informático visado de eventuais acessos não autorizados, através de meios semelhantes.

Finda a investigação, é redigido um relatório detalhado, a fim de assegurar o exercício do contraditório, onde constem: (1) os meios técnicos utilizados; (2) a duração da investigação; (3) as características do sistema informático; (4) o estado em que se encontrava antes da investigação; (5) as alterações sofridas após o acesso; (6) os dados recolhidos; e (7) a unidade policial que executou a técnica.

Fora do âmbito do § 20k da Lei para a Defesa Face aos Perigos do Terrorismo Internacional, a jurisprudência alemã tem interpretado as secções 100a e seguintes do StPO, relativas à interceção de telecomunicações, no sentido de admitir o recurso ao *malware,* nos casos em que haja necessidade de aceder a conversas automaticamente encriptados, ou seja, admite-se a instalação de *software* malicioso, a fim de desencriptar as mesmas[127].

Em suma, com base nos requisitos indicados pelo Tribunal Constitucional Federal Alemão, foi introduzido no ordenamento jurídico uma norma que permite o recurso ao *malware*, ainda que em caso excecionais, isto é, se um outro meio menos lesivo não for suficiente para obter o mesmo resultado, e apenas em casos de repressão das infrações *supra* referidas ou de prevenção, designadamente de terrorismo internacional.

3.2.2 Espanha

Até 2015, o recurso ao *malware*, como meio de obtenção de prova em processo penal, não estava previsto no ordenamento jurídico espanhol. Contudo, ao longo dos anos, a jurisprudência ao sustentar-se nas regras das tradicionais buscas foi admitindo o mesmo, o que levou o TEDH a condenar o Estado espanhol[128].

---

[127] Cf. MIRJA GUTHEIL *et al*., *Legal Frameworks for*..., op. cit., p. 79.
[128] Cf. DAVID SILVA RAMALHO, «O uso de *malware*...», pp. 220-221, e JUAN CARLOS ORTIZ PRADILLO, «El *Remote Forensic*…», op. cit., p. 6.

Apesar de o projeto de lei para a reforma da *Ley de Enjuiciamiento Criminal* existir desde 2011[129], só em 8 de dezembro de 2015 é que a nova *Ley de Enjuiciamiento Criminal*[130] entrou em vigor.

Esta introduziu no seu Título VIII, no Capítulo IX, no artigo 588 *septies a.*, uma norma que prevê a possibilidade de recurso ao *malware* como meio de obtenção de prova[131], isto é, a instalação de um *software* que permita via remota e telemática o exame à distância, sem conhecimento do seu titular ou do utilizador do conteúdo de um computador, dispositivo eletrónico, sistema informático, instrumento de armazenamento em massa de dados informáticos ou base de dados.

Este meio só poderá ser autorizado pelo juiz, e caso estejamos perante um crime do catálogo, ou seja: crimes cometidos no seio de organizações criminosas; crimes de terrorismo; crimes contra menores ou incapazes; crimes contra o Estado e a defesa nacional; e crimes cometidos por meio de um sistema informático ou qualquer outra tecnologia de informação ou telecomunicação ou serviço de comunicação.

O despacho do juiz deve especificar: (1) os sistemas informáticos ou os dispositivos técnicos que serão acedidos, bem como os meios de armazenamento de dados informáticos ou base de dados, dados ou outros conteúdos digitais objeto da investigação; (2) o âmbito em que é realizada esta técnica e o modo a que se procederá ao acesso e apreensão dos dados ou ficheiros informáticos, e o *software* através do qual se executará o controlo da informação; (3) os agentes autorizados para executar o meio; (4) o despacho de autorização, caso haja, para a realização e conservação de cópias dos dados informáticos; e (5) as medidas necessárias para a preservação, autenticidade, integridade, inacessibilidade ou supressão de dados armazenados no sistema informático acedido.

Quanto ao período de duração, o recurso a este meio encoberto não poderá exceder os três meses.

Em suma, estes artigos apenas vieram dar forma ao que já estava previsto no *Projecto Gallardón*, o qual tinha como objetivo demonstrar a necessidade de uma

---

[129] Cf. JUAN CARLOS ORTIZ PRADILLO, *Problemas Procesales de la Ciberdelincuencia*, Madrid, Editorial Colex, 2013, p. 193.

[130] No dia 8 de dezembro de 2015, foi notícia, no *El País*, a possibilidade de uso de *malware*. Cf. JOSÉ MANUEL ABAD LIÑÁN, «La Policía podrá instalar un troyano en el ordenador de sospechoso», *El País*, 08-12-2015, disponível em http://tecnologia.elpais.com/tecnologia/2015/12/04/actualidad/1449259283_679909.html [consultada a 06-10-2016].

[131] Poderá consultar o mesmo em http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725 [consultado a 06-10-2016].

regulamentação que procurasse o equilíbrio entre a capacidade do Estado em fazer frente a este novo tipo de criminalidade e o direito à privacidade e ao sigilo nas comunicações.

3.2.3 Estónia

Desde de janeiro de 2013, o ordenamento jurídico do país também prevê o uso de *malware*, como meio de obtenção de prova em processo penal[132]. Esta possibilidade está prevista no Capítulo 3.1, sob a epígrafe atividades de vigilância, designadamente no § 126.3, número (5) do *Kriminaalmenetluse seadustik* (CPP)[133].

Este meio encoberto só poderá ser utilizado: para fins de prevenção criminal; fins de repressão criminal; execução de uma decisão que recaia sobre uma pessoa fugitiva; ou em caso de necessidade de recolha de informações previstas nos § 403 e seguintes do CPP. Porém, para que este meio possa ser utilizado, previamente deverá ter-se tentado recolher prova através dos meios previstos no § 126.3, números (1), (2) e (3). Assim, o recurso ao *malware* só é admitido quando: não for possível recolher dados e provas através de outros meios; for impossível recolher dados e prova em prazo razoável; for especialmente difícil; ou prejudicar os interesses da investigação.

Quanto ao catálogo de crimes, o mesmo está previsto no § 126.2, número (2) e é diversificado, como, entre outros: crimes contra a Humanidade; ordem, tranquilidade e paz pública; identidade cultural; integridade pessoal; património cultural; segurança internacional; vida; integridade física; liberdade pessoal; e liberdade e autodeterminação sexual.

Também se encontra previsto um catálogo de sujeitos no § 126.2, número (3). Só é possível utilizar este meio contra pessoa: da qual se tenham motivos sérios e justificáveis para acreditar que se prepara para cometer um dos crimes do catálogo; em fuga; que detenha bens objeto de confisco; seja suspeita ou arguida num processo já iniciado; que haja sérios e justificados motivos para crer que cometeu um crime do catálogo; e que comunique, transmita informações, auxilie ou seja proprietário do meio de comunicação utilizado pelo suspeito.

A atividade de vigilância ao sistema informático pode ser realizada mediante autorização do Ministério Público ou juiz de investigação preliminar. O juiz de

---

[132] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 301.

[133] Poderá acompanhar o mesmo em http://www.legislationline.org/documents/section/criminal-codes [consultado a 06-12-2016].

instrução preliminar decidirá com base no requerimento fundamentado do Ministério Público e o juiz de inquérito preliminar deve rever o pedido e autorizar ou não a realização da técnica.

Quanto ao prazo de duração, o § 126.4, número (6) prevê que é de um ano, podendo, em casos excecionais, ser superior a isso.

Finda a operação, deverá ser elaborado um relatório onde conste a entidade/pessoa que a realizou, hora e local da sua efetivação, identificação da pessoa visada, data do despacho de autorização, data de apresentação do pedido, identificação dos dados recolhidos essenciais para a descoberta da verdade, e um anexo com os registos da operação. Por sua vez, os dados recolhidos devem ser guardados em ficheiro especial.

O sujeito alvo da técnica é notificado, finda a mesma, exceto nos casos previstos no § 126.13, número (2), nomeadamente: quando resulte prejuízo para o processo; numa violação dos direitos fundamentais; e perigo para outra pessoa envolvida ou para a confidencialidade do método ou tática usada.

Em conclusão, apesar do *malware* estar previsto neste ordenamento jurídico, aplicam-se as regras gerais para as atividades de vigilância. Por outras palavras, não existe um catálogo de crimes e sujeitos especial para este meio oculto, como também não existe um prazo específico nem um procedimento a seguir para esta técnica em particular. Nenhum dos artigos do Capítulo 3.1 descreve concretamente em que consiste este meio, aliás, o mesmo é introduzido numa alínea em que se prevêem outros locais/objetos sujeitos à vigilância. Não há nenhuma norma em especial que faça alusão a este meio oculto com as demais consequências.

Salvo melhor opinião, apesar de estarem verificados os requisitos que também se observaram nos ordenamentos vizinhos, estes são usados em termos gerais para o *malware*, sem ter em consideração as particularidades deste meio de obtenção de prova.

3.2.4 Finlândia

Desde janeiro de 2014, no ordenamento jurídico finlandês está previsto o uso de *malware*, como meio de obtenção de prova em processo penal[134]. Esta possibilidade

[134] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 301.

está regulada na Lei das Medidas Coercivas (806/2011)[135], designadamente no Capítulo 10, secção 23 e seguintes.

É permitida a vigilância técnica do sistema informático utilizado pelo suspeito de cometer um dos crimes do catálogo. Isto significa que um agente de investigação criminal pode instalar um dispositivo ou programa para a vigilância do sistema, caso as necessidades da investigação assim o exigem. Para este fim, o agente pode aceder secretamente ao sistema informático, instalar, retirar, ou utilizar um dispositivo, procedimento ou programa, desinstalar ou de outro modo impedir ou dificultar, temporariamente, a proteção do sistema visado.

Quanto aos crimes que admitem o recurso a este meio encoberto, fazem parte do catálogo: (1) aqueles cuja pena aplicável em abstrato é de, pelo menos, quatro anos de prisão; (2) os relacionados com o tráfico de drogas; (3) a preparação de atos terroristas; (4) os de falsificação de moeda e título de crédito graves; (5) a preparação de tomada de reféns; e (6) a preparação de um crime grave contra a propriedade. Pode recorrer-se quer em casos de prevenção quer em casos de repressão criminal.

A competência para decretar o recurso cabe ao juiz, mediante requerimento da autoridade policial com poder de detenção. O despacho de autorização para utilizar o *malware* deverá especificar: o crime que se investiga e a data em que foi cometido; identificar o suspeito; os factos com base nos quais a pessoa é suspeita e que preenchem os requisitos para o recurso a este meio; a duração, com a data exata em que termina; o sistema informático que será vigiado; a pessoa que executará e que supervisionará; e, por fim, as possíveis restrições e condições para a sua utilização.

Já no que se refere ao prazo, esta técnica só poderá ter a duração máxima de um mês, renovável por igual período.

Face ao exposto, concluímos que neste ordenamento jurídico falta uma norma indicativa do procedimento a adotar. Com efeito, a secção 26 remete para as buscas domiciliárias, sem qualquer outra especificação. Na nossa opinião, esta remissão cabe nos casos em que é necessário instalar um dispositivo físico para aceder ao sistema informático, tal como acontece no ordenamento jurídico francês, como veremos.

[135] A mesma está disponível para consulta em http://www.finlex.fi/en/laki/kaannokset/2011/en20110806.pdf [consultada a 06-12-2016].

3.2.5 França

No âmbito da *Loi d'orientation et de programmation pour la performance et la sécurité intérieure* (Loppsi)[136], foram tomadas várias medidas relacionadas com a cibercriminalidade, designadamente, houve a necessidade de bloquear certos *websites*[137] e vigiar determinados suspeitos.

Esta lei introduziu, nos artigos 706-102-1 a 706-102-9 do CPP[138], a possibilidade de a polícia judiciária aceder aos dados informáticos do visado – quer os que já estão gravados, como os que aparecem no ecrã e os dados que vão sendo introduzidos ou recebidos pelo visado em tempo real –, gravá-los, recolhê-los ou transmiti-los. Existindo duas possibilidades legais: (1) acesso remoto a partir da instalação física de *malware* no sistema informático alvo; e (2) acesso remoto a dados, iniciados remotamente[139].

Ora, desde essa data, o recurso ao *malware* é admitido em duas situações: (1) em caso de necessidade de inquérito; e (2) em caso de necessidade de informações, mas apenas para os crimes previstos nos artigos 706-73 e 706-73-1 do CPP, *ex vi* artigo 706-102-1. Neste caso: crimes como os de homicídio qualificado cometidos por grupo organizado; tortura e outros tratamentos cruéis, degradantes ou desumanos cometidos por grupo organizado; tráfico de estupefaciente e de pessoas; sequestro e rapto cometidos por grupo organizado; lenocínio; roubo cometido por grupo organizado; extorsão; destruição, degradação e deterioração de bens cometidos por grupo organizado; contrafação de moeda ou de títulos equiparados; terrorismo; tráfico de armas e produtos explosivos; auxilio à entrada, circulação e residência de um estrangeiro em França; branqueamento; associação criminosa; omissão de rendimentos;

---

[136] Em português significa lei de orientação e de programação para o desempenho e a segurança interna (Lei n.º 2011-267, de 14 de março de 2011). No seguimento da Loppsi, houve várias notícias sobre a possibilidade de a polícia judiciária utilizar *malware.* Cf. GUILLAUME CHAMPEAU, «LOPPSI: l'installation de mouchards chez les suspects est adoptée», *Numerama*, 11-02-2010, disponível em http://www.numerama.com/magazine/15076-loppsi-l-installation-de-mouchards-chez-les-suspects-est-adoptee.html [consultada a 11-10-2016], SANDRINE COCHARD, «Loppsi 2: comment le gouvernement veut-il surveiller nos ordinateurs?», *20 Minutes*, 29-01-2014, disponível em http://www.20minutes.fr/high-tech/383386-20100209-loppsi-2-comment-gouvernement-veut-il-surveiller-ordinateurs [consultada a 09-10-2016], GUILLAUME CHAMPEAU, «La PJ pourra enfin installer des keyloggers et autres mouchards», *Numerama*, 04-03-2016, disponível em http://www.numerama.com/politique/150304-la-pj-pourra-enfin-installer-des-keyloggers-et-autres-mouchards.html [consultada a 09-10-2016].

[137] Por exemplo, os prestadores de serviço de *internet* foram notificados para bloquear *sites* públicos com conteúdo pedo-pornográfico.

[138] Em 3 junho de 2016, os artigos 702-102-1 a 706-102-8 sofreram alterações com a Lei n.º 2016-731, a qual reforçou a luta contra o crime organizado, o terrorismo e o seu financiamento e aperfeiçoou a eficácia e as garantias do procedimento penal.

[139] Cf. MIRJA GUTHEIL *et al.*, *Legal Frameworks for...*, op. cit., p. 73.

captura ou desvio de aeronave, navio, comboio ou veículo de transporte coletivo por grupo organizado; atividades perigosas para o ambiente cometidas por grupo organizado e fraude perpetuada por grupo organizado. Dito de outro modo, o catálogo cobre a criminalidade grave e organizada e o terrorismo, havendo apenas uma referência ao cibercrime.

No que se refere à competência, cabe ao: (1) juiz das liberdades e da detenção; ou (2) juiz de instrução.

Na primeira hipótese, o juiz das liberdades poderá, mediante requerimento do Ministério Público, autorizar os oficiais ou os inspetores da polícia judiciária indicados pelo Procurador da República a instalar, fisicamente, um dispositivo técnico, sem consentimento do visado, com o intuito de recolher dados. Para o efeito, o Procurador da República nomeará qualquer pessoa, singular ou coletiva, habilitada e inscrita na lista oficial para efetuar as operações técnicas necessárias à elaboração do dispositivo técnico, ou em alternativa prescrever o recurso a meios do Estado submetidos ao segredo da defesa nacional, nos termos do Capítulo I, do Título IV, do Livro I (artigo 706-102-1).

Na segunda hipótese, o juiz de instrução, após consulta ao Ministério Público, autorizará os oficiais ou inspetores da polícia judiciária em comissão rogatória a instalar, fisicamente, um dispositivo técnico, sem consentimento do visado, com o intuito de recolher dados. Também designará qualquer pessoa, singular ou coletiva, habilitada e inscrita na lista oficial para efetuar as operações técnicas necessárias à elaboração do dispositivo técnico, ou prescreverá o recurso a meios do Estado submetidos ao segredo da defesa nacional, nos termos do Capítulo I, do Título IV, do Livro I (artigo 706-101-2).

Em ambos os casos, o despacho deverá ser fundamentado, sob pena de nulidade, indicando os crimes em causa, a localização ou descrição detalhada do sistema informático e a duração da operação (1.ª parte do artigo 706-102-3).

No que diz respeito ao prazo de duração: na primeira situação (a requerimento do Procurador da República), é de um mês, renovável uma vez por igual período, desde que se verifiquem os respetivos requisitos de admissibilidade; na segunda situação (por iniciativa do juiz de instrução), é de quatro meses, renovável por igual período, desde que a duração total das operações não exceda o limite máximo de dois anos (artigo 706-102-3).

Em termos de procedimento, as operações são realizadas sob a autoridade e controlo de quem as concedeu, ou seja, do Ministério Público ou do juiz de instrução, os quais poderão ordenar a todo o tempo a sua interrupção (artigo 706-102-4). A instalação e a desinstalação do dispositivo técnico deverão ocorrer nos termos e condições dos artigos 706-102-5 e 706-102-6. Prevê o artigo 706-102-5 a proteção de determinadas profissões ou grupos profissionais, por estarem abrangidos pelo segredo profissional.

Finda a operação, o juiz de instrução ou o oficial ou inspetor da polícia judiciária, escolhido por ele ou indicado pelo Procurador da República, realizará um relatório de cada uma das operações de instalação do dispositivo técnico e das operações de recolha dos dados informáticos. Este relatório deve mencionar a data e a hora em que a operação começou e terminou (artigo 706-102-7).

Os dados recolhidos são guardados e selados. O juiz de instrução ou o oficial ou inspetor da polícia judiciária descreve ou transcreve no relatório do processo os dados que são úteis à descoberta da verdade, não podendo ser guardado nenhum dado relativo à vida privada do visado e estranho ao processo (artigo 706-102-8). No fim do prazo de prescrição da acusação, os dados informáticos são destruídos, por ordem do Procurador da República ou do Procurador-Geral, sendo elaborado um relatório da operação de destruição (artigo 706-102-9).

Em conclusão, até à entrada desta lei, apenas estava previsto no artigo 706-96 do CPP a recolha secreta, através de dispositivo técnico, de som em locais ou veículos privados ou públicos, ou de imagem em local privado. Com a entrada em vigor da *Loppsi*, a polícia tem a possibilidade de recolher em tempo real dados informáticos, mas sempre em casos excecionais. Da letra da lei, subentende-se que a intenção do legislador é permitir o recurso a este meio encoberto em casos de repressão "necessidades do inquérito" e em caso de prevenção "necessidades de informação". No entanto, do ponto de vista de duração da técnica, com o devido respeito, somos da opinião que o prazo aplicado a cada um deles não é coerente, isto porque é de quatro meses nos casos de prevenção e, de um mês, nos casos de repressão.

À semelhança do ordenamento jurídico alemão, o normativo francês também satisfaz os requisitos indicados pelo Tribunal Constitucional Federal alemão, ou seja: prevê a fase do processo; a competência; o prazo; o catálogo de crimes e sujeitos; e o procedimento.

É também de saudar que este meio oculto só deverá ser instalado fisicamente no sistema informático[140] do visado por um perito, para que posteriormente a polícia possa instalar à distância um *software* malicioso a fim de monitorizar a atividade do suspeito, evitando que outros sistemas informáticos que não o do visado sejam infetados. Contudo, tem a desvantagem de só ser permitida a sua utilização no caso de se conhecer a localização física do sistema.

A grande preocupação na utilização deste meio é a garantia da cadeia de custódia dos dados recolhidos. Atualmente, não existem disposições legais que prevejam este desafio, e o procedimento não é uniforme. Existem apenas princípios gerais que devem ser seguidos para assegurar a integridade da prova recolhida[141]. Refere a juiz francesa, Emmanuelle Legrand, no estudo do Parlamento Europeu, que os juízes não são informados das técnicas e métodos utilizados na realização da operação, dificultando o controlo da legalidade[142]. Por fim, também os juízes e os procuradores não têm conhecimento suficiente para o seu uso, nem têm acesso a essas ferramentas técnicas[143].

3.2.6 Itália

Os órgãos de investigação criminal italianos têm recorrido, nos últimos anos, ao uso de *malware* como meio de obtenção de prova em processo penal. Embora este meio oculto ainda não esteja regulado no seu ordenamento jurídico[144], para o efeito, aplicam analogicamente o disposto com vista à interceção das comunicações.

O Acórdão do Supremo Tribunal de Cassação, divisão V, decisão número 24695, datado de 14 de outubro de 2009, permitiu o recurso ao *malware* para apreender e copiar documentos que se encontravam num disco rígido, sem um mandado de busca. O mesmo considerou que esta técnica não consistia na vigilância, porém na apreensão e cópia de documentos guardados no disco rígido do sistema informático do arguido, não envolvendo qualquer processo de comunicação, mas sim um processo comunicativo entre o processador e o sistema eletrónico[145]. Por assim ser, entendeu que não haveria

---

[140] Daí, compreender-se que a técnica mais usada seja o *keylogger*. Cf. MIRJA GUTHEIL *et al*., *Legal Frameworks for*…, op. cit., p. 76.
[141] Cf. *Ibidem*, p. 74.
[142] Cf. *Ibidem*, p. 75.
[143] Cf. *Ibidem*, p. 73.
[144] Cf. MIRJA GUTHEIL *et al*., *Legal Frameworks for*..., op. cit., p. 84.
[145] Cf. GIUSEPPE VACIAGO e DAVID SILVA RAMALHO, «Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings», *Digital Evidence and Electronic Signature Law Review*, volume 13, novembro de 2016, p. 91.

necessidade de um mandado de busca do juiz encarregado das investigações preliminares para o uso deste meio encoberto[146].

Em 2012, o Acórdão do Tribunal de Cassação, divisão VI, decisão número 254865, datado de 27 novembro, confirmou esta resolução, referindo que apenas era necessária uma ordem do Ministério Público[147].

Já em 2015, o Acórdão do Tribunal de Cassação, divisão VI, decisão número 27100, datado de 26 maio, entendeu em sentido contrário, considerando que este tipo de técnica se enquadrava na vigilância eletrónica, pelo que deviam estar verificados determinados pressupostos, nomeadamente a identificação do sistema informático e a sua localização[148].

Ora, face às discrepâncias jurisprudenciais, esta matéria foi discutida, em julho de 2016, nas Sessões Conjuntas do Supremo Tribunal de Cassação Italiana, decisão n.º 1. No debate estava a possibilidade de realizar a vigilância eletrónica entre presentes com recurso à instalação deste género de ferramentas nos sistemas informáticos dos visados, mesmo no seu domicílio e sem que a atividade criminosa tenha recorrido ao sistema informático.

Concluíram as Sessões Conjuntas que este meio oculto só poderá ser usado em casos de criminalidade particularmente grave, nomeadamente, crimes organizados, terrorismo, nos termos do artigo 51 (3-bis) do Código de Processo Penal Italiano, e que a vigilância através da instalação de *malware* não tem em consideração o local onde se encontra o sistema informático, tornando a vigilância eletrónica aleatória[149].

Esta decisão ainda distinguiu a busca *online* da vigilância *online*. Considerou, para o efeito, que a primeira consistia na possibilidade de fazer uma cópia, total ou parcial, das unidades de memória do sistema informático visado, sendo os dados e informações transmitidos em tempo real aos órgãos de investigação criminal. A segunda possibilidade correspondia a um modo de interceção de fluxos de informação, o que permitia a interceção dos dados transmitidos pelo microfone, *webcam*, teclado, entre outros. Ou seja, era possível o controlo remoto em tempo real de tudo o que era exibido na tela, no teclado (através de *keylogger*) e a gravação das conversas (através do microfone) e vigilância (através da *webcam*)[150].

---

[146] Cf. *Ibidem*.
[147] Cf. *Ibidem*, p. 92.
[148] Cf. *Ibidem.*
[149] Cf. *Ibidem*.
[150] Cf. *Ibidem*.

Face à inexistência de um enquadramento jurídico, nos últimos anos, têm sido várias as propostas legislativas com o intuito de regular o uso de *malware*[151]. A última proposta de lei foi apresentada em fevereiro de 2017, denominando-se de "Projeto de Lei Quintarelli". Este Projeto[152] visa introduzir um novo meio de investigação – *Osservazione e acquisizione da remoto* (busca remota e apreensão) –, aplicando ao *malware* as disposições já existentes em matéria de meios de investigação criminal.

Propõe o Projeto de Lei que a competência para autorizar a técnica de *malware* seja do juiz que presidir a investigação preliminar, mediante requerimento do Ministério Público, e que este meio apenas seja utilizado se for indispensável e nenhum outro garantir o mesmo resultado.

Esta autorização deve especificar as funções que serão utilizadas pelo *software*. Significa isto que, deverão existir vários tipos de *software* malicioso, cada um com determinadas potencialidades, e no momento da autorização deve ser especificado qual se irá utilizar.

Quanto ao catálogo de crimes, deverão os mesmos referir-se apenas à criminalidade organizada. Já no que diz respeito aos sujeitos e aos locais estes devem ser especificados.

Propõem também o Projeto que após a recolha dos dados, os mesmos sejam guardados nos servidores do Ministério Público de forma encriptada e todos os dados que não sejam relevantes para o crime que se investiga devem ser eliminados.

Quanto ao procedimento, deve caber aos órgãos de polícia criminal, excluindo-se imediatamente empresas privadas. Durante a operação, deverá ser elaborado um relatório, onde se regista e documenta todas as ações, com o intuito de permitir o exercício do contraditório. Finda a investigação, deverá o *malware* ser eliminado com segurança do sistema informático, e o sujeito visado notificado.

Por fim, prevê este Projeto que cada *malware* deverá ser certificado e registado numa "Comissão Nacional de *Malwares*" com determinado número de série e versão. Anualmente, os *malwares* à disposição dos órgãos de investigação devem ser revistos

---

[151] Em 2015, também já tinha sido discutida a possibilidade de consagração deste meio encoberto. Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., pp. 299-300.

[152] A este propósito, consultar o resumo da proposta de alteração do Código de Processo Penal Italiano em http://www.civicieinnovatori.it/wp-content/uploads/2017/02/Sintesi-PDL-captatori-EN.pdf [consultado a 02-12-2017].

por uma entidade competente, com o intuito de se certificarem das suas funções, garantido o cumprimento da lei.

Face ao exposto, a grande preocupação dos especialistas nesta matéria prende-se com a garantia da cadeia de custódia, a recolha de prova noutras jurisdições e a falta de conhecimento por parte dos advogados, o que poderá pôr em causa o exercício do contraditório.

Como podemos observar, embora grande parte dos pressupostos seja comum a todos os Estados-Membros analisados, os seus parâmetros de aplicação são diferentes.

Este meio oculto, na generalidade dos regimes, poderá ser utilizado para fins de prevenção e repressão criminal, mas sempre em casos excecionais, ou seja, se for impossível ou muito difícil alcançar o mesmo resultado com meios menos lesivos.

Quanto à competência, em regra, cabe ao juiz[153], mediante requerimento do órgão que investiga, devendo o despacho ser fundamentado, com base em determinados critérios. Só no ordenamento jurídico alemão é que é permitido o recurso ao *malware*, sem autorização judicial prévia em casos excecionais, mas deve ser requerido posteriormente no prazo de três dias.

Relativamente ao conteúdo do despacho, é variável, mas, por regra, deve detalhar o âmbito, os requisitos, a razão pela qual este meio é utilizado, os crimes em causa, o sujeito visado, o sistema informático, a duração e os agentes autorizados para executar este método. Ao contrário do que se esperava, só o ordenamento espanhol é que se preocupou em detalhar no despacho de autorização o modo em que se procede ao acesso e apreensão dos dados ou ficheiros informáticos, assim como o *software* através do qual se executa, o controlo da informação e as medidas necessárias para a preservação, autenticidade, integridade, inacessibilidade ou supressão de dados armazenados no sistema informático acedido.

No que se refere ao catálogo de crimes, uma vez mais este é diferente de regime para regime jurídico, porém sempre com um crime em comum – o terrorismo. No nosso entendimento, o catálogo da Estónia é exagerado face ao grau de lesão deste meio oculto. Salvo melhor opinião, consideramos que os regimes jurídicos mais ponderados, e que possivelmente poderiam ser fonte de inspiração para o ordenamento português,

[153] No ordenamento jurídico alemão, cabe ao presidente do tribunal.

são o espanhol, o alemão e o francês, pese embora este último admita crimes com uma pena de prisão de dois anos, aplicável em abstrato.

A duração deste meio também é muito diferente; temos prazos máximos de um mês a um ano. Na Finlândia, o prazo é de um mês; em França, varia entre um e quatro meses, conforme seja da iniciativa do órgão que investiga ou do juiz; na Alemanha e em Espanha, o prazo é de três meses e, na Estónia, de um ano. Consideramos, com o devido respeito, que o prazo razoável seria de um mês.

Por último, referimos que em certos regimes são de saudar determinados requisitos. Assim vejamos.

Nos ordenamentos jurídicos alemão, espanhol e francês, há o cuidado de descrever detalhadamente em que consiste o recurso ao *malware*. Não obstante, só o alemão garante o mínimo de alterações possíveis no sistema informático e que as mesmas sejam reversíveis, bem como a técnica utilizada deva garantir a proteção do sistema informático de meios semelhantes. Por sua vez, o francês e o finlandês optam por este meio encoberto só poder ser instalado fisicamente.

Quanto aos dados recolhidos, só o ordenamento jurídico alemão prevê que os mesmos devem ser analisados pela comissão de proteção de dados e pelo juiz, para se certificarem de que não dizem respeito ao núcleo essencial da vida privada[154]. Considerámos também importantíssimo o requisito da elaboração de um relatório para o exercício do contraditório, como acontece na Alemanha e na Estónia.

Por fim, o Projeto de Lei italiano tem como ponto positivo a distinção das potencialidades de cada tipo de *malware* que pode ser utilizado, evitando, assim, o arbítrio por parte dos órgãos de investigação criminal.

Em conclusão, os pressupostos essenciais num regime jurídico são: (1) a fase do processo; (2) a autorização judiciária fundamentada; (3) o catálogo de crimes; (4) a duração da técnica; (5) a notificação do sujeito; e (6) a elaboração de relatórios.

[154] Embora tenha sido considerada inconstitucional, esta triagem e supressão de dados são um passo positivo. Com as alterações sugeridas pelo tribunal, isto é, que a triagem seja feita por um órgão independente, este pressuposto será uma forte proteção para os dados privados.

4. A legitimidade do recurso ao *malware*

Como referiu MANUEL DA COSTA ANDRADE[155], até há duas décadas atrás, o processo penal evoluiu para um processo de estrutura acusatória, com espaço aberto para o princípio da investigação criminal, construído sobre o dogma da dignidade e integridade do arguido, onde se privilegiavam a liberdade e as garantias de defesa em detrimento da eficácia na descoberta da verdade e na perseguição criminosa. Hoje, este paradigma está em crise, face ao enfraquecimento de conceitos e princípios basilares do processo penal do Estado Liberal, ao constante ampliar dos dispositivos que legitimam a compressão dos direitos fundamentais, às forçosas interpretações da lei e às novações jurisprudências, entre outras causas.

Todavia, não significa isto que o processo penal, ao combater as novas realidades emergentes da evolução tecnológica e social, tem legitimidade para deixar de garantir o menor grau de lesão possível de direitos, liberdades e garantias. Na verdade, "*o Estado e os seus órgãos terão tanta mais legitimidade – e só assim a terão – para exercerem a ação penal e para exercitarem o poder punitivo quanto mais respeitadores dos direitos, liberdades e garantias dos cidadãos mostrarem e quanto mais as suas decisões se impuserem ao respeito da comunidade e forem compreensíveis para o Povo.*"[156].

Portanto, em matéria de métodos ocultos de investigação, o que se impõe é uma ponderação entre direitos, princípios e valores conflituantes. É precisamente aqui que se encontra o desafio e a irresistibilidade[157]. Ou seja, como é quase impossível a existência de um processo penal eficaz sem a restrição de direitos constitucionalmente garantidos, deverá procurar-se um equilíbrio entre o interesse do Estado na prossecução penal e a tutela adequada dos direitos dos cidadãos. Dito de outro modo, estamos perante um sacrifício que o Estado estará disposto a fazer em matéria de direitos fundamentais e processuais penais, para a prossecução penal dos delinquentes[158] ou para a prevenção, mas deverá fazê-lo tendo em consideração certos vetores.

Ora, como observámos nos capítulos antecedentes, o *malware* constitui um portentoso meio de obtenção de prova. Dentre as principais características, refiram-se: a

---

[155] Ver «Métodos ocultos de investigação…», op. cit., pp. 525-528.
[156] Cf. ANTÓNIO GARCIA PEREIRA, «Breves reflexões sobre o estado presente do Processo Penal em Portugal», *in* Manuel Monteiro Guedes Valente (coord.), *III Congresso de Processo Penal*, Coimbra, Almedina, 2010, p. 207.
[157] Cf. RITA CASTANHEIRA NEVES, *As Ingerências nas Comunicações*…, op. cit., p. 95.
[158] Cf. *Ibidem*, p. 160.

omissão e anulação de alguns direitos processuais convencionais do arguido, como o direito à não autoincriminação; a neutralização do direito a não prestar depoimento por parte de certas testemunhas a que se arroga; a incidência sobre um grande número de sujeitos; a recolha de enorme quantidade e qualidade de dados[159]; e a lesão de um vasto leque de direitos fundamentais. Assim, revela-se mais intrusivo, quando comparado com os clássicos métodos encobertos. Porém, potencialmente, será um meio bastante útil na prossecução da justiça. Posto isto, coloca-se a pergunta se a extrema eficácia deste meio é suficiente para a sua justificação.

Neste capítulo, embora de modo não aprofundado por este estudo se revelar insuficiente, propomo-nos efetuar a análise da legitimidade da utilização do *malware* em processo penal. Apresentaremos os direitos fundamentais e processuais penais possivelmente sacrificados, as razões da necessidade de recurso a este método e, numa segunda fase, demonstraremos em que termos é possível a sua restrição.

4.1 A intromissão nos direitos fundamentais

Do que foi estudado anteriormente, parece-nos que o *malware* como meio de obtenção de prova pode contender com vários direitos, designadamente: direito à reserva da intimidade (n.º 1 do artigo 26.º da CRP, artigo 7.º da Carta dos Direitos Fundamentais da União Europeia, e artigo 8.º da Convenção Europeia dos Direitos do Homem); direito à palavra ou à voz (n.º 1 do artigo 26.º da CRP); direito à imagem (n.º 1 do artigo 26.º da CRP); direito à inviolabilidade do domicílio (n.º 1 do artigo 34.º da CRP, artigo 7.º da Carta dos Direitos Fundamentais da União Europeia, e artigo 8.º da Convenção Europeia dos Direitos do Homem); direito ao segredo das comunicações (n.º 4 do artigo 34.º da CRP, artigo 7.º da Carta dos Direitos Fundamentais da União Europeia, e artigo 8.º da Convenção Europeia dos Direitos do Homem); direito à autodeterminação informacional; e ao novo direito à integridade e confidencialidade dos sistemas informáticos, como veremos.

Assim, de modo breve, referiremos o teor de cada um destes direitos.

---

[159] A propósito da vigilância das telecomunicações, HANS-JÖRG ALBRECHT tinha concluído de forma semelhante. Cf., deste autor, «Vigilância das telecomunicações. Análise teórica e empírica da sua implementação», *Que Futuro Para o Direito Processual Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, coord. Mário Ferreira Monte *et al.*, Coimbra, Coimbra Editora, 2009, p. 726.

4.1.1 Direito à reserva da intimidade

O direito à reserva da intimidade traduz-se em distintas dimensões, pois é possivelmente um dos direitos que tem maior alcance prático[160]. Numa perspetiva simplista, compreende não apenas o direito de oposição à divulgação da vida privada, mas também ao seu respeito. Caracteriza-se pela capacidade de impedir o acesso de estranhos a informações sobre a vida privada e familiar, e o direito a que ninguém divulgue as mesmas. O âmbito normativo deste direito deve delimitar-se no conceito de "vida privada" que tenha em conta três aspetos: o respeito dos comportamentos; o respeito do anonimato; e o respeito da vida em relação[161].

O Tribunal Constitucional[162], em abundante jurisprudência, tem concretizado o alcance deste direito. Das decisões proferidas, verifica-se que o direito à intimidade tem uma amplitude definida casuisticamente. Assim, não podemos afirmar que este direito começa no ponto A e termina no ponto B. Contrariamente, atrevemo-nos a dizer que o seu âmbito de aplicação é quase ilimitado e, em consequência, não permite uma definição precisa do mesmo. Acresce referir, não ser o local um critério decisivo para demarcar o que está incluído na vida privada[163].

Por sua vez, em matéria de obtenção de prova para a prossecução da justiça penal, encontram-se limites constitucionais expressos na vida privada. Designadamente, não são permitidas buscas ao domicílio ou ingerências na correspondência, nas telecomunicações e demais meios de comunicação, por se traduzirem numa abusiva intromissão na vida privada[164].

Em síntese, a reserva da vida privada "*assume na doutrina dos direitos fundamentais e dos correspondentes bens jurídicos pessoais: proteção contra a indiscrição e devassa arbitrárias das "coisas" (segredos, espaços, eventos, vivências,*

---

[160] Cf. JORGE MIRANDA e RUI MEDEIROS, *Constituição Portuguesa Anotada*, tomo I, Coimbra, Coimbra Editora, 2005, p. 290.
[161] Cf. J. J. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, 4.ª edição revista, volume I, Coimbra, Coimbra Editora, 2007, p. 468. (2014)
[162] Para um estudo mais aprofundado, ver PAULO MOTA PINTO, «A proteção da vida privada na jurisprudência do Tribunal Constitucional», *Jurisprudência Constitucional*, número 10, abril/junho de 2006, Coimbra, Coimbra Editora, pp. 12-28, e MARIA FERNANDA PALMA, «Tutela da vida privada e processo penal – realidades e perspectivas constitucionais», *Jurisprudência Constitucional*, número 10, abril/junho de 2006, Coimbra, Coimbra Editora, pp. 3-12.
[163] Cf. PAULO MOTA PINTO, «A proteção da vida privada…», op. cit., p. 19.
[164] Cf. JORGE MIRANDA e RUI MEDEIROS, *Constituição Portuguesa Anotada*, op. cit., p. 291.

emoções e experiências) que a pessoa quer legitimamente reservar para si e para aqueles que elege para o efeito."[165].

Por último, importa alertar que o direito à intimidade também está relacionado com o direito à inviolabilidade do domicílio e direito à imagem. Porém, estes direitos são passíveis de autonomia.

No caso do recurso ao *malware* como meio de obtenção de prova, o direito à reserva da intimidade é comprimido, grosso modo, por dois motivos. Primeiro, porque a utilização de *software* malicioso permite a ativação da *webcam* e do microfone do sistema informático do suspeito ou arguido. Significa isto, que é possível capturar, em tempo real, tudo o que se passa na sua intimidade, ou seja podemos encontrá-lo na mais 'brutal' e espontânea privacidade. Em segundo lugar, porque o sistema informático ao guardar uma colossal quantidade e qualidade de dados, como compras e vendas, planificação de negócios, contabilidade, movimentos bancários, trabalhos realizados, escritos íntimos (ou não), fotografias, vídeos, exames e relatórios médicos, correspondência, entre outros, funciona como uma biblioteca, um repositório, ou um diário, pelo que é o espelho do indivíduo[166].

4.1.2 Direito à palavra

Apesar de o direito à palavra, assim como à imagem, ter nascido a partir do direito à reserva da intimidade, atualmente, é consensual na nossa doutrina a sua plena autonomização[167]. Este direito, como também o da imagem, é expressão típica da autonomia e da identidade pessoal constitucionalmente garantida. Inclui o poder de domínio, isto é o direito a que não sejam registadas ou divulgadas palavras da pessoa sem o seu consentimento, conferindo desta forma um direito à "reserva" e à "transitoriedade" da palavra falada (no sentido da convicção do titular de que a mesma é apenas ouvida naquele momento exato)[168].

---

[165] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 155, e JORGE MIRANDA e RUI MEDEIROS, *Constituição Portuguesa Anotada,* tomo I, 2.ª edição, Coimbra, Coimbra Editora, 2010, pp. 619-622.

[166] Neste mesmo sentido, ver MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 167.

[167] Cf. JOÃO GOUVEIA DE CAIRES, «O registo de som e imagem e as escutas ambientais», *in Direito da Investigação Criminal e da Prova*, coord. Maria Fernanda Palma *et al*., Coimbra, Almedina, 2014, p. 276.

[168] Cf. JORGE MIRANDA e RUI MEDEIROS, *Constituição Portuguesa Anotada*, op. cit. (2.ª edição), p. 618.

Ora, esta proteção implica a salvaguarda da "integridade de uma esfera privada" de comunicação verbal, através da garantia da confidencialidade das palavras não publicamente gravadas, mesmo que não se refiram à intimidade da vida pessoal ou familiar. Este direito até se pode considerar parte do direito à autodeterminação informacional, sendo proibidas as gravações e escutas de conversas privadas sem conhecimento e consentimento da pessoa em causa, bem como a proibição da montagem/deformação ou utilização das palavras de determinada pessoa.

Em síntese, o direito à palavra desdobra-se em três: (1) direito à voz, pelo que é ilícito, sem o consentimento do cidadão, registar e divulgar a sua voz; (2) direito às palavras ditas, pelo que elas não podem ser retiradas do seu contexto; e (3) direito ao auditório, ou seja escolher o círculo de pessoas a quem é transmitida a palavra[169]. Objetiva-se tanto o resguardo frente ao exterior, como ao Estado ou a qualquer entidade pública e privada.

4.1.3 Direito à imagem

O direito à imagem inscreve-se na representação da figura da pessoa, bem como a sua interação com o exterior, protegendo-se a autonomia e a identidade pessoal[170]. Ou seja, implica a proteção contra o registo da imagem, quer por fotografia quer por vídeo, como a sua reprodução/mostragem e difusão. Cada pessoa poderá decidir da utilização ou não deste tipo de registos que incidem sobre si[171].

Em resumo, é o direito a definir a sua própria auto-exposição, o direito a não ser fotografado nem de ver a sua imagem exposta sem o seu consentimento, assim como o direito a não ver apresentada sob qualquer modo a sua imagem de forma ofensiva ou malevolamente distorcida ou infiel[172]. Traduz-se no direito a controlar a utilização dos registos da sua imagem e, consequentemente, o direito à autodeterminação da imagem exterior. À semelhança do direito à palavra, visa o resguardo em relação ao exterior, ao Estado e a qualquer entidade pública e privada.

Com a utilização de *software* malicioso em processo penal, o direito à palavra e à imagem estão postos em causa. Com efeito, este meio de obtenção de prova além de

---

[169] Cf. J. J. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, op. cit., p. 467.
[170] Cf. JOÃO GOUVEIA DE CAIRES, «O registo de som e imagem…», op. cit., p. 277.
[171] Cf. JORGE MIRANDA e RUI MEDEIROS, *Constituição Portuguesa Anotada*, op. cit. (2.ª edição), p. 618.
[172] Cf. J. J. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, op. cit., p. 467.

permitir o acesso a todo o conteúdo do sistema informático, nomeadamente, gravações, vídeos, fotografias e outras formas de reprodução da palavra e da imagem, sem o consentimento nem o conhecimento do seu utilizador ou proprietário, também permite a gravação de voz e a captura de fotografias e vídeos, em tempo real, através da ativação da *webcam* e do microfone, sem que o utilizador se aperceba disso. Em nosso entender, há também uma manifesta violação do direito à palavra, através da utilização de *keyloggers*, na medida em que a entidade investigadora tem acesso a tudo o que é digitado pelo utilizador ou proprietário do sistema informático, incluindo as palavras que escreveu e acabou por apagar e não enviar. Esses dados, embora não transmitidos ou reproduzidos, não podem deixar de estar englobados neste direito.

4.1.4 Direito à inviolabilidade do domicílio

Quanto ao direito à inviolabilidade do domicílio, é difícil definir o seu alcance[173]. Considerado o sentido constitucional, entende-se por domicílio o local onde se habita, independentemente de ser habitação permanente, temporária, principal ou secundária, bem como o local de trabalho, conforme os artigos 82.º e 83.º do Código Civil[174]. De modo resumido, como considerou já o Tribunal Constitucional, é um "*espaço fechado e vedado a estranhos, onde recatada e livremente se desenvolve toda uma série de condutas e procedimentos característicos da vida privada e familiar*"[175]. Por sua vez, todas as pessoas físicas que habitem na residência estão protegidas por este direito, independentemente das relações jurídicas subjacentes.

Por último, acresce referir, tal como entendem J. J. GOMES CANOTILHO e VITAL MOREIRA, que "*o domicílio não é violado somente quando se entra na morada de alguém sem o seu consentimento. [Também os] modernos meios técnicos [existentes] possibilitam a invasão e devassa do domicílio mediante meios eletrónicos, que, além disso, permitem também a devassa das conversas e da vida privada dos moradores. [Logo, a] inviolabilidade do domicílio é seguramente incompatível com tais mecanismos*" [176].

---

[173] Assim, JORGE MIRANDA e RUI MEDEIROS, *Constituição Portuguesa Anotada*, op. cit. (2.ª edição), pp. 758-761.
[174] Considerou o Tribunal Constitucional, a título de exemplo, que os segmentos habitacionais dos grupos e as caravanas de pessoas nómadas como objeto de direito à inviolabilidade de domicilio. Cf. MARIA FERNANDA PALMA, «Tutela da vida privada…», op. cit., p. 9.
[175] Cf. *Ibidem*.
[176] Ver *Constituição da República Portuguesa Anotada*, op. cit., p. 541.

Ora, com a utilização de *malware*, poderemos estar perante uma violação deste direito. Nos dias de hoje, o sistema informático – quer seja um telemóvel, *tablet* ou portátil –, permite-nos recorrer às suas funcionalidades em qualquer local, isto é, na rua, em casa ou no trabalho. Por conseguinte, a entidade investigadora poderá estar a invadir o direito à inviolabilidade do domicílio, por exemplo, se aceder ao sistema informático quando este se encontre no lar do suspeito ou arguido. Acresce, ainda, que não é só o sujeito processual que é lesado com este método. Com a ativação do *hardware*, também haverá devassa das conversas e da vida privada dos restantes moradores.

4.1.5 Direito ao segredo das comunicações

O direito ao segredo das comunicações inclui a proibição de ingerência das autoridades públicas nos meios de comunicação. Este direito abrange toda a espécie de correspondência e de telecomunicações entre pessoas, não apenas quanto ao conteúdo, mas também relativamente aos dados de tráfego, ou seja, espécie, data, hora e duração, entre outros.

No nosso caso, sem dúvida, este direito poderá vir a ser comprimido, pelos motivos já expostos, como a possibilidade de ativação do microfone e, posteriormente, a oportunidade de se ouvir, por exemplo, conversas telefónicas, e o acesso em tempo real às comunicações.

4.1.6 Direito à autodeterminação informacional

O direito à autodeterminação informacional surgiu após a Decisão dos Censos (*Volkszählung*)[177]. Ela foi um marco para a história da proteção de dados pessoais, pois colocou o indivíduo no centro do processo informacional, com direito a conhecer e a consentir o tratamento de dados que lhe dizem respeito.

A fundamentação do tribunal baseou-se no direito geral da personalidade, previsto no n.º 1 do artigo 2.º, em conjugação com o n.º 1 do artigo 1.º, ambos da Lei Fundamental de Bona, garantindo ao cidadão a proteção contra a recolha, armazenamento, uso e transmissão ilimitados de dados pessoais, exceto em caso de interesse geral da comunidade, mas sempre quando fundamentado na Constituição e na

[177] Cf. BVerfGE, 65,1, disponível em http://www.servat.unibe.ch/dfr/bv065001.html [consultada a 26-03-2017]. Não foi esta Decisão que lhe deu origem, mas proporcionou debates futuros nessa matéria.

lei[178]. A Decisão pretendeu criar uma barreira normativa contra as tendências para transformar o indivíduo num mero objeto informacional[179].

Por sua vez, a doutrina passou a explicar o direito à autodeterminação informacional como um "*ciclo onde coexistem os direitos à "autodeterminação" (Selbstbestimmung), à "autopreservação" (Selbstbewharung) e à "autoapresentação" (Selbstdarstellung)*"[180].

Por último, esta resolução também foi importante no sentido de se abarcar direitos que não encontram expressão na Constituição, no direito geral da personalidade. O tribunal reconheceu que este último direito pode adquirir um significado diferente, considerados os novos perigos resultantes da evolução tecnológica para a tutela de direitos.

Significa isto que, dada a quantidade e a qualidade de informação contida num sistema informático, o recurso ao *malware* também viola o direito à autodeterminação informacional, pois possibilita traçar, sem qualquer esforço, o perfil do seu utilizador.

4.1.7 Direito à integridade e confidencialidade dos sistemas informáticos

Concretamente relacionado com a utilização de *malware*, surgiu na Alemanha um novo direito fundamental.

O Acórdão do Tribunal Constitucional Federal Alemão, de 27 de fevereiro de 2008, sobre o direito à integridade e confidencialidade dos sistemas informáticos (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*), surgiu quando foi introduzido o § 5.2 (11) na Lei de Proteção da Constituição da Renânia do Norte-Vestefália, em 20 de dezembro de 2006, com intuito de permitir à *Bundesamt für Verfassungsschutz* (entidade competente) a instalação de *malware* e o acesso secreto a sistemas informáticos.

Diante desta norma, três requerentes apresentaram um recurso constitucional invocando a violação direta dos seus direitos constitucionais. Apesar de nenhum deles ter sido alvo de uma investigação criminal, demonstraram que a sua atividade profissional poderia ser erroneamente interpretada e, consequentemente, os seus sistemas informáticos alvos de uma pesquisa remota, o que violaria os seus direitos

[178] Cf. ALEXANDRE SOUSA PINHEIRO, *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa, AAFDL Editora, 2015, p. 479.
[179] Cf. *Ibidem*, p. 486.
[180] Cf. *Ibidem*, p. 478.

fundamentais[181]. Um dos reclamantes era jornalista e, no âmbito da sua atividade, acedia a *sites* da *internet* administrados por pessoas com visões extremistas e com conexões com organizações igualmente extremistas, participando também nos *chats* hospedados nesses *sites*, não obstante o seu computador ser também utilizado para fins pessoais[182]. O segundo reclamante era membro de um partido político que estava sob observação da entidade responsável pela proteção da Constituição, e usava o seu computador para fins profissionais e privados[183]. Por último, o terceiro reclamante, que era advogado e ajudava requerentes de asilo, alguns dos quais sob vigilância da referida entidade, também utilizava o seu computador no âmbito profissional e pessoal[184].

O tribunal ao admitir o recurso inteirou-se dos problemas que este método oculto poderia levantar. Concluiu que, subjacente ao meio, estava em causa uma grande quantidade de dados que permitia traçar o perfil do utilizador do sistema informático.

Delimitada esta questão, o tribunal avançou, posteriormente, com a análise do recurso ao *malware* como meio de obtenção de prova, à luz dos seguintes direitos fundamentais: direito ao segredo das telecomunicações; direito à inviolabilidade do domicílio; e direito à autodeterminação informacional.

O tribunal verificou que o n.º 1 do artigo 10.º da GG (direito ao segredo das telecomunicações) não protegia os dados guardados no sistema informático, depois de concluído o processo de comunicação, ou seja, os dados relativos a uma determinada comunicação que se encontrassem já armazenados. Isto porque, nesse caso, já tinha cessado o perigo decorrente da comunicação à distância, que este direito tutela. Concluiu, assim, que o n.º 1 do artigo 10.º da GG apenas estaria corretamente enquadrado, se o meio em causa se limitasse à recolha de comunicações em curso na rede ou a informações com as mesmas relacionadas[185].

O tribunal passou, então, a analisar o problema face ao direito à inviolabilidade do domicílio, nos termos do artigo 13.1 da GG, que visa proteger a esfera espacial dentro da qual a vida privada do cidadão decorre, face à intromissão física de terceiros. Começou, desde logo, por referir que este direito também tutela ingerências efetuadas a

---

[181] Cf. WIEBKE ABEL e BURKHARD SCHAFER, «The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822», *SCRIPTed – A Journal of Law, Technology & Society*, volume 6, número 1, abril de 2009, p. 110.
[182] Cf. *Ibidem*, p. 110.
[183] Cf. *Ibidem*.
[184] Cf. *Ibidem*.
[185] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., pp. 217-218.

partir do exterior (sem a intromissão física no domicílio), ou seja protege o cidadão da monitorização ótica e acústica, assim como da monitorização do sistema informático através da mediação da radiação eletromagnética. Por fim, este direito não se esgota no domicílio do sujeito, abrangendo também o espaço onde o mesmo desenvolve a sua atividade comercial ou profissional.

No entanto, o tribunal acabou por concluir que no caso do acesso remoto a um sistema informático, localizado no domicílio do visado, com o intuito de ativar o microfone ou a *webcam* e, posteriormente, capturar a informação dentro do espaço das quatro paredes – ou no caso de entrada no domicílio do visado e consequente acesso ao sistema informático aí localizado –, estaríamos perante uma restrição ao direito à inviolabilidade do domicílio. Contrariamente à tese apresentada pelo Governo (que defendeu a posição supracitada), o tribunal considerou que estávamos perante uma questão diversa: o acesso remoto a um sistema informático com o intuito de espiar, controlar, monitorizar e analisar os dados aí armazenados. Por um lado, porque este método de obtenção de prova poderia ser utilizado independentemente da localização do sistema informático e, por outro, a localização podia ser desconhecida pela entidade que investiga. Assim, se estivesse em causa o direito à inviolabilidade do domicílio, o mesmo seria inútil caso o sistema informático se encontrasse fora do espaço privado. Referiu, a título de exemplo, o caso em que um sujeito começa a escrever um *e-mail* no seu domicílio, edita-o no banco do jardim público e envia-o quando regressa a casa. Na mesma atividade, a pessoa estaria sucessivamente protegida e desprotegida por este direito, em virtude da proteção alternar consoante o suspeito ou arguido se encontre num espaço privado ou público[186], conferindo-se, assim, tutelas distintas aos mesmos dados e sistemas informáticos decorrentes da sua localização.

Acresce notar que, atualmente, esta análise faz todo o sentido pois é cada vez mais frequente a utilização de dispositivos móveis, isto é, *tablets*, *smartphones* e portáteis, entre outros, pelo que não podemos ficar 'ancorados' a uma proteção que tem em si implícita a localização do sistema. A mobilidade é uma característica destes novos aparelhos informáticos, que permitem receber e enviar informações em qualquer parte do mundo.

Verificada mais uma lacuna, o tribunal prosseguiu a sua análise de acordo com o direito à autodeterminação informacional. Como referido, este direito foi cunhado por

[186] Cf. WIEBKE ABEL e BURKHARD SCHAFER, «The German Constitutional Court…», op. cit., p. 116.

via jurisprudencial, partindo do direito ao livre desenvolvimento da personalidade e do direito à dignidade da pessoa humana, conferindo ao utilizador o poder de disposição dos seus dados pessoais.

O Governo Regional da Renânia do Norte-Vestefália tinha concluído que o direito à autodeterminação se aplica ao recurso ao *malware*. Porém, tal como o tribunal veio a determinar, o mesmo não oferece proteção adequada perante a criação automática de dados gerados pela mera utilização dos sistemas informáticos. Estes sistemas permitem armazenar grandes quantidades de informação (fotografias, vídeos, dados bancários, dados relativos à saúde, contabilidade e correspondência, entre outros), mas é o cidadão quem escolhe se pretende ou não armazená-los. Pelo contrário, no caso dos dados criados automaticamente pelo próprio sistema e altamente sensíveis, estes não se encontram no poder de disposição do cidadão o que, por sua vez, leva a que não fiquem protegidos pelo direito à autodeterminação informacional. Logo, a entidade que acede ao sistema pode recolher informação sensível e privilegiada do utilizador, que já se encontra processada, sem necessidade de outro tipo de tratamento, podendo com ela traçar o perfil do seu titular. Assim, o tribunal reconheceu a gravidade que o acesso secreto a um sistema informático representa para a personalidade do sujeito, o qual excede o âmbito de tutela do direito à autodeterminação informacional.

Mediante estas conclusões, o tribunal compreendeu que os direitos constitucionais existentes não eram suficientes para proteger o sujeito, face à intromissão do *malware* no seu núcleo privado. Existia, portanto, uma lacuna geral de proteção, diante dos riscos emergentes do uso de sistemas informáticos para o desenvolvimento da personalidade dos seus utilizadores.

Nesse sentido, o tribunal adivinhou a necessidade de reconhecimento da existência de um direito fundamental emergente do direito previsto no artigo 2.1 da GG, conjugado com o artigo 1.1 da mesma lei. Este novo direito deveria tutelar, adequadamente, a vida privada dos cidadãos contra acessos do Estado na área da tecnologia da informação, em especial, quando desse modo se tenha acesso total aos dados armazenados no sistema informático[187].

Posto isto, o tribunal cunhou um novo direito fundamental – o direito à integridade e confidencialidade dos sistemas informáticos (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*). O

[187] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 220.

mesmo visa proteger, por um lado, o interesse do utilizador do sistema em garantir que os dados criados por si ou gerados automaticamente, tratados e armazenados pelos sistemas informáticos, permaneçam confidenciais e, por outro, que a integridade do sistema não seja comprometida através de acessos não autorizados por parte de terceiros.

Naturalmente, de modo obrigatório, previu que um sistema informático sob tutela do direito à sua integridade e confidencialidade necessita de ter capacidade de só por si ou através de ligação à rede armazenar ou conter, em quantidade e qualidade, dados pessoais do visado suscetíveis de o caracterizar. Isto é, deve permitir que, a partir do seu acesso, a entidade que investiga consiga traçar o perfil do utilizador.

Reconheceu, também, que o sistema informático não necessita de conter dados, mas sim ter capacidade para estar ligado à rede (por exemplo, à *internet*) permitindo, desta forma, o acesso aos mesmos. Assim, este direito protege igualmente os sistemas que sejam acessíveis através daquele sistema informático, isto é, os *webmails* e os serviços de computação em 'nuvem', entre outros.

Por último, considerou que o direito à integridade e confidencialidade do sistema informático aplica-se, da mesma forma, nos casos em que se recorre ao uso de *keyloggers*, uma vez que, apesar de não se tratar de aceder aos dados em si, está a monitorizar-se tudo o que é digitado no teclado do sistema informático.

Em suma, acabou o tribunal por concluir que o § 5.2 (11) da Lei de Proteção da Constituição da Renânia do Norte-Vestefália violava o direito à integridade e confidencialidade dos sistemas informáticos, bem como os princípios da proporcionalidade, da clareza e certeza legal, pelo que se pronunciou pela sua inconstitucionalidade.

Ora, feitas estas referências, podemos aferir que o uso de *malware* em processo penal lesa, pelo menos, direitos como: à palavra, à imagem; à intimidade[188]; e à integridade e confidencialidade dos sistemas informáticos.

4.2 A violação dos princípios do processo penal

Feita a decomposição na perspetiva constitucional, passaremos agora a confrontar a utilização deste método encoberto ante as garantias processuais do sujeito.

[188] Segundo JOÃO GOUVEIA DE CAIRES, «O registo de som e imagem…», op. cit., p. 277, o direito à imagem e à palavra poderá estar em sobreposição com o direito à reserva da vida privada.

4.2.1 Princípio da audiência e defesa

Este princípio encontra a sua consagração nos n.ºs 1 e 7 do artigo 32.º da CRP e implica que nenhuma decisão que atinja a esfera jurídica da pessoa possa ser tomada sem que lhe seja dada a possibilidade de ser ouvida. Em consequência, relativamente aos meios de prova, a pessoa deve poder controlar as provas oferecidas pela acusação ou produzidas oficiosamente[189].

Podemos, de certa forma, considerar que, no caso do recurso ao *malware* como meio oculto de obtenção de prova, este princípio será eventualmente ferido. Chegámos a esta conclusão, ao atender que a utilização de meios encobertos para recolha de prova não é, frequentemente, dada a conhecer ao arguido ou ao suspeito. Pelo que, após a ingerência, a pessoa continua na ignorância, o que implica o desconhecimento da verdadeira origem de determinados meios de prova carreados para os autos.

Mediante as duas realidades invocadas, as pessoas afetadas não poderão opor-se, quer antes quer depois, nem fazer valer a ilegalidade por violação de qualquer dos pressupostos legais. Mesmo que venham a tomar conhecimento posteriormente, a devassa é irreversível[190].

4.2.2 Princípio do contraditório

Ao invés da violação do princípio que acabámos de referir, poderá também entender-se que o que está em causa é o contraditório (n.º 5 do artigo 32.º da CPR). Ou seja, a possibilidade de, em situação de igualdade de armas, ser feita contraprova. Isto porque, na senda do que referimos anteriormente, pode o sujeito não ser informado do modo como foi recolhida a prova ou qual o *malware* utilizado, pelo que seria impossível a sindicância e verificação da fidedignidade da prova recolhida[191].

4.2.1 Princípio do julgamento justo e equitativo

Relativamente a este princípio, a sua maior expressão encontra-se no *nemo tenetur se ipsum accusare*. Ou seja, ninguém pode ser obrigado a contribuir para a sua própria incriminação, o que engloba o direito ao silêncio e o direito de não facultar meios de prova, tendo estes a sua base, nomeadamente, na alínea d) do n.º 1 do artigo 61.º, alínea a) do n.º 4 do artigo 141.º, n.º 1 do artigo 343.º, e n.º 1 *in fine* do artigo

---

[189] Cf. PAULO DE SOUSA MENDES, *Lições de Direito Processual Penal*, 3.ª reimpressão, Coimbra, Almedina, 2015, p. 207.
[190] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 107.
[191] Neste sentido, veja-se DAVID SILVA RAMALHO, «O uso de *malware*…», op. cit., p. 236.

345.º, todos do CPP. Na verdade, o que está em causa são garantias processuais do arguido ou do suspeito, tal como os direitos fundamentais e a dignidade da pessoa humana.

Ora, é por demais evidente que, com o recurso ao meio encoberto que nos propusemos retratar, este princípio se encontra beliscado. Tivemos oportunidade de ver que além da recolha de uma grande quantidade de dados, este método oculto permite a captura, em tempo real, de imagem/vídeo, som e palavras escritas. Consequentemente, o arguido ou o suspeito, ou mesmo terceiras pessoas, continuam a falar, a agir e a fazer coisas inconscientemente, contribuindo para a sua incriminação e facilitando os meios de prova.

4.2.2 Direito a recusar testemunho ou depoimento

Salvo melhor opinião, também está em causa o direito a recusar o depoimento (artigos 132.º, n.º 2, 134.º e 135.º do CPP), na medida em que o recurso aos meios ocultos não assegura a tutela do mesmo. Este direito tem na sua essência o "*prevenir formas larvadas e indiretas de auto-incriminação, preservar a integridade e a confiança nas relações de maior proximidade familiar, proteger o alargado espectro de valores individuais e supra-individuais pertinentes à área de tutela da incriminação da violação de segredo profissional ou de segredos para efeitos equivalentes […], poupar as pessoas concretamente envolvidas às situações dilemáticas de conflito de consciência de ter de escolher entre mentir ou ter de contribuir para a condenação de familiares ou clientes*."[192].

4.3 O outro prato da balança

Observados os principais direitos e princípios lesados, resta-nos, agora, verificar se existem 'argumentos' que justificam o recurso a este meio encoberto, apesar do mesmo se revestir de um elevado nível de danosidade. Note-se que não iremos elencar exaustivamente os fatores que legitimam a imprescindibilidade do emprego de *malware* como meio de obtenção de prova, pois podem ser vários; iremos só referir alguns dos principais argumentos apontados.

Em primeiro lugar, e como indigita DAVID SILVA RAMALHO[193], este meio oculto é necessário para fazer frente ao surgimento de programas informáticos que têm

[192] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 110.
[193] Cf. DAVID SILVA RAMALHO, «O uso de *malware*…», op. cit., pp. 208-212.

como único objetivo dificultar a recolha de prova e, consequentemente, a imputação das atividades ilícitas ao seu autor. Ou seja, referimo-nos às medidas anti-forenses. Estas têm como intuito evitar a existência de prova ou esconder e manipular a existente, no sentido de não ser acessível à entidade que investiga. Dentre as medidas anti-forenses utilizadas, podemos referir três[194].

Em primeiro lugar, conforme analisámos no capítulo terceiro, estão os *softwares* de anonimização, por exemplo o *Tor*, que permitem esconder *online* o 'rasto' da atividade até ao seu verdadeiro autor.

Em segundo lugar, a esteganografia, a cifragem de dados e a limpeza do disco. A esteganografia caracteriza-se por ocultar informação de qualquer tipo de ficheiro eletrónico (documentos e imagens, entre outros), através da alteração ou introdução de informação, o que permite esconder em ficheiros aparentemente inofensivos outros ilegais. Quanto à criptografia, qualifica-se como a introdução de uma chave num ficheiro, tornando-o ilegível. Dito de outro modo, e como vimos no capítulo anterior, estamos perante o caso dos ficheiros encriptados em que é necessário o conhecimento da palavra-passe para acedermos aos mesmos. No que diz respeito à *data wiping*, esta possibilita eliminar todos os dados de um sistema informático através da sucessiva gravação sobre os mesmos. Por outras palavras, a limpeza do disco permite gravar por cima da informação outra aleatória. Assim, quando se fizer uma pesquisa informática ou cópia integral desse sistema – no contexto de recolha de prova – não se detetam aqueles ficheiros.

Em terceiro lugar, o problema também se coloca nas próprias ferramentas com que se efetuam as perícias forenses e a recolha de prova digital. O uso das mesmas assenta no pressuposto de que a recolha de prova não será afetada pela sua presença ou utilização. Acontece que têm surgido medidas com o objetivo de ativar mecanismos de reação, ou seja a falsificação ou modificação da prova quando está a ser recolhida, o que perturba a fidedignidade da mesma em sede de julgamento.

Por estas razões, as medidas anti-forenses, que são cada vez mais frequentes, constituem uma preocupação atual. A utilização de *malware*, como meio de obtenção de prova, permitiria contorná-las.

---

[194] Em sentido mais desenvolvido, ver DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., pp. 128-152.

Como vimos nos capítulos anteriores, a instalação de *software* malicioso num sistema informático, por parte dos órgãos de polícia criminal, possibilita a obtenção de informações que não seriam recolhidas de outra forma, designadamente a localização do sistema informático. Permite, também, monitorizar a atividade daquele sistema, o que facilita o conhecimento de ficheiros onde se recorreu à estenografia ou cifragem. Noutra perspetiva, através da instalação de *keylogger*, é possível recuperar a palavra-passe de ficheiros encriptados. Por fim, o facto de ser um método oculto 'desarma' o utilizador, pois este desconhece que está a correr uma investigação contra si, estando assim menos precavido.

O recurso a este método oculto também se mostra indispensável na perseguição e repressão das novas formas de criminalidade contemporânea. A criminalidade altamente organizada, o terrorismo e o terrorismo internacional, entre outros, pelas suas próprias características, são quase um santuário imune à devassa dos meios tradicionais e "abertos" de investigação, como refere MANUEL DA COSTA ANDRADE. Este tipo de criminalidade, além de mobilizar meios sem precedentes e possuir um poder inconcebível, opta por formas de organização e de interação que tornam as suas atividades isentas à intromissão e devassa das instâncias de controlo. Acresce que este tipo de criminalidade organizada se caracteriza por relações de mais consenso do que de conflito. Portanto, também não é habitual procurarem a solidariedade da ordem jurídica, pelo contrário, há aqui uma solidariedade recíproca[195].

Por seu turno, algumas formas de crime fazem um uso extensivo da tecnologia de informação. Deste modo, se não recorrermos a este tipo de métodos ocultos, não seremos capazes de combater em pé de igualdade essas atividades criminosas. A especial gravidade dos ilícitos criminais e a sofisticação do seu modo de execução, quando revelam a insuficiência dos meios existentes para lhes fazerem frente[196], justificam a consagração e recurso ao *malware*, o que por si só também é mais gravoso e sofisticado.

Como último fator, podemos referir o facto de os meios de obtenção de prova, em geral, estarem pensados para um mundo físico, isto é, para prova física. Acontece que eles não se adaptam à nova realidade do mundo virtual, ou seja, da prova digital.

---

[195] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 106, e ID., «Métodos ocultos de investigação…», op. cit., p. 535.
[196] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 178.

Em consequência, a eficácia destes meios desenhados para o mundo 'real' não é a mesma quando aplicada a esta nova realidade binária.

Assim, a opção do legislador não pode passar por ficar de braços cruzados, a assobiar para o lado, como se não se apercebesse que estes meios não se aplicam à nova realidade. Em suma, não pode querer que o 'vestido' que foi costurado para uma determinada pessoa assente "como uma luva" noutra pessoa com um corpo completamente distinto. Ora, é precisamente isso que se tem verificado nos últimos anos, relativamente à obtenção de prova digital. Insiste-se em colocar naquele 'vestido um corpo que não lhe pertence'. Por esse motivo, este método oculto surge também como necessário, eventualmente entre outros.

4.4 A ponderação

Mercê do nível de danosidade do *malware*, a sua utilização não seria admissível, à partida, como meio de obtenção de prova em processo penal. No entanto, não podemos chegar a uma conclusão tão 'radical', excluindo, desde logo, todas as hipóteses de utilização. Os fins do processo penal, a descoberta da verdade, a realização da justiça, o restabelecimento da paz jurídica (comunitária) e a proteção dos direitos fundamentais, são bens de igual peso. Por conseguinte, impõe-se uma ponderação.

Na verdade, o que se observa é o dever do Estado – perante a evolução social e tecnológica e o surgimento de novas formas de criminalidade –, em garantir a segurança dos cidadãos e combater a delinquência. Recorrendo às palavras de MARIA FERNANDA PALMA, estamos perante dois apelos: um à preservação de um espaço íntimo de livre realização de si mesmo e de expressão da respetiva identidade; e outro, aparentemente antagónico, de proteção da segurança e de realização da justiça em matéria de Direito Processual Penal, que reclama intrusão, exposição e controlo da pessoa pelo sistema jurídico[197].

É neste equilíbrio, como afirma JORGE DE FIGUEIREDO DIAS[198], que reside a tarefa legislativa e doutrinal do presente e do futuro. O legislador, não obstante ter de estar atento aos ditames constitucionais, não pode deixar de prestar atenção às

---

[197] Cf. MARIA FERNANDA PALMA, «Tutela da vida privada e processo penal (soluções para o conflito de valores na jurisprudência constitucional)», *in Estudos em Memória do Conselheiro Luís Nunes de Almeida*, Coimbra, Coimbra Editora, 2007, p. 656. Neste contexto, a autora dá o exemplo da utilização de diários íntimos ou outros documentos privados, em que a recolha da prova em processo penal se faz à custa de uma intromissão na vida íntima, nomeadamente nas confidências e reflexões que o arguido realiza em momentos anteriores à prática do crime.

[198] Ver, deste autor, «O Processo Penal Português: Problemas e Prospectivas», op. cit., p. 809.

exigências e à celeridade impostas pela evolução e, consequentemente, ao surgimento de novos e mais eficazes meios de investigação para, quando for necessário, intervir através de legislação.

Na opinião de JORGE REIS NOVAIS, o não considerar a possibilidade de restringir os direitos fundamentais, quando em colisão com outros bens constitucionais, teria como reverso a não observância ilegítima de outras normas constitucionais face a situações de conflito[199]. Ora, os 'choques' de valores constitucionais são situações caracterizadas pela circunstância da CRP proteger e tutelar valores que por si podem ser conflituantes[200], sendo necessário, nestes casos, resolver o conflito com base numa ponderação. Logo, estamos perante "*a necessidade de equilíbrio da tensão entre a exigência, por uma parte, de manutenção do processo penal como um sistema de sólida garantia de direitos fundamentais do cidadão, e por outra parte, de abertura ao tratamento eficiente de formas expansivas, massificadas, altamente organizadas e definitivamente internacionalizadas de criminalidade gravíssima*"[201].

Neste caso, vistos os bens em conflito, somos da opinião que os direitos fundamentais em apreço devem 'ceder' perante a necessidade da segurança dos cidadãos e de punição dos criminosos. Ou seja, defendemos que o *malware* como meio oculto de obtenção de prova é legítimo. Para o efeito, deverá obedecer às exigências constitucionais.

4.5 A execução do equilíbrio

A legitimidade do recurso a este meio oculto deve ser erigida sob os critérios fornecidos pela Constituição. Numa primeira fase, na estruturação do regime jurídico e, num segundo tempo, na autorização da ingerência no caso concreto.

Mais abaixo, ainda que de modo não exaustivo, tentaremos identificar os princípios fundamentais que devem ser observados para que seja legítima a utilização e escolha do *malware* como meio de obtenção de prova em processo penal.

---

[199] Cf. JORGE REIS NOVAIS, *As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição*, Tese de Doutoramento em Ciências Jurídico-Políticas, Faculdade de Direito da Universidade de Lisboa, 2002, volume II, p. 502. (policopiada)

[200] Cf. NUNO LUMBRALES, «Direitos fundamentais: o direito à palavra, o direito à imagem e a prova audiovisual em processo penal», *Revista do Ministério Público do Rio Grande do Sul*, número 67, setembro/dezembro de 2010, p. 219.

[201] Cf. JORGE DE FIGUEIREDO DIAS, «O Processo Penal Português: Problemas e Prospectivas», op. cit., p. 809.

4.5.1.1 Princípio da reserva de lei

Excluímos, desde logo, a hipótese de utilização de *malware*, nos termos do artigo 125.º do CPP, porque esta técnica é um novo meio de obtenção de prova. Ora, a admissão deste meio oculto não poderá decorrer da aplicação analógica do regime previsto para um outro meio encoberto[202], porque a subsunção de outros meios, por via judicial e não só, aos regimes consagrados para outros, implica uma substituição ilegítima do aplicador da lei ao legislador. Como refere MANUEL DA COSTA ANDRADE[203], as leis existentes não podem ser vistas como normas penais em branco, ou seja, com plasticidade suficiente para se adaptar aos novos meios técnicos de invasão e devassa. Ao contrário do que acontece com os direitos fundamentais, que com o progresso tecnológico expandem ou emergem, independentemente de ser pela expansão e densificação da área de tutela de um direito fundamental já existente ou pela autonomização de um novo e nominado direito fundamental. Os novos meios de investigação, designadamente o *malware* como método oculto, configuram um sacrifício para os direitos fundamentais e devem estar sujeitos a uma intransponível exigência de reserva de lei, nos termos dos n.ºs 2 e 3 do artigo 18.º e alínea b) do artigo 165.º da CRP[204]. Dito de outro modo, o *malware* só é admissível e válido se e na estrita medida em que gozar de expressa e específica consagração legal[205].

Esta exigência é uma condição fundamental da legitimidade e da validade da prova obtida através dele. Só desta forma é que se previne o abuso e o arbítrio das atuações da autoridade judiciária no emprego deste método, pois sujeitamo-los ao estrito cumprimento dos pressupostos legais que foram consagrados. Portanto, a norma

---

[202] As próprias características deste método afastam a possibilidade da aplicação analógica a meios que foram pensados para uma realidade física.

[203] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 113.

[204] Recorde-se que prescrevendo os n.ºs 2 e 3 do artigo 18.º da CRP o regime constitucional da restrição de direitos, a sua legitimidade depende da verificação de certos pressupostos. A restrição deve estar expressamente prevista na constituição, deve salvaguardar outros direitos ou interesses constitucionalmente protegidos, não pode aniquilar o direito em causa com a diminuição da extensão e do alcance essencial do respetivo preceito, a própria lei terá de ter caráter geral e abstrato, não pode ter efeitos retroativos e deverá revestir de caráter de lei da Assembleia da República ou decreto-lei autorizado. Cf. salientam, MANUEL MONTEIRO GUEDES VALENTE, «Terrorismo e Processo Penal: Uma Relação Amarga (?)!», *in* Manuel Monteiro Guedes Valente (coord.), *II Congresso de Processo Penal*, Coimbra, Almedina, 2006, pp. 168-173; MARIA DE FÁTIMA MATA-MOUROS, *Juiz das Liberdades. Desconstrução de um mito do processo penal*, Coimbra, Almedina, 2011, p. 209; JORGE REIS NOVAIS, *As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição*, 2.ª edição, Coimbra, Coimbra Editora, 2010, p. 727, ou ainda J. J. GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, op. cit., pp. 374-396.

[205] Cf. MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação…», op. cit., p. 540.

terá de prever, de modo expresso e explícito, a medida de compressão dos direitos fundamentais, bem como definir os seus limites.

Nesta tarefa, exige-se clareza, determinabilidade e densificação do regime jurídico. Por um lado, porque só assim se permitem a compreensão e o conhecimento que possibilitem a adaptação das condutas dos visados. Por outro, permite-se o controlo efetivo do emprego deste método, ou seja, dá-se ao lesado a possibilidade de sindicar a legalidade e validação da prova obtida através dele, na medida em que conhece as 'regras' que deveriam ter sido observadas.

Quer isto dizer que a norma deve delimitar o uso de *malware*, prescrevendo os pressupostos para a sua utilização. Se assim não for, estamos a criar um normativo em branco que abre portas ao livre-arbítrio do seu aplicador, o que por si não é compatível com o grau de danosidade deste meio de obtenção de prova.

Como refere MANUEL DA COSTA ANDRDADE, deverá respeitar-se um conjunto combinado de variáveis: catálogo de crimes; grau de suspeita; subsidiariedade; autorização/ordenação por autoridade competente; e informação da pessoa atingida depois de terminada a medida. Ou seja, o regime jurídico do *malware* terá de desenhar os pressupostos gerais a que deve obedecer a aplicação deste meio[206]. As variáveis acima referidas são gradativamente mais exigentes, quando comparadas com as que existem para outros métodos ocultos.

Em suma, o que se pretende é a existência de um diálogo entre o legislador penal e o legislador constitucional para, posteriormente, existir um outro diálogo entre o juiz e a Constituição[207].

Para além de se exigir reserva de lei, o regime jurídico do *malware* deverá ser construído assente no princípio da proibição do excesso ou, como lhe preferimos chamar, da proporcionalidade em sentido amplo.

4.5.1.2 Princípio da proporcionalidade

O princípio da proporcionalidade é uma referência para atuação dos poderes públicos em Estado de Direito, assumindo no que diz respeito a direitos fundamentais um papel de instrumento de controlo da atuação restritiva da liberdade individual. Está previsto no n.º 2 do artigo 29.º da DUDH, e faz depender os limites aos direitos e às liberdades das "*justas exigências da moral, da ordem pública e do bem-estar numa*

[206] Cf. MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação…», op. cit., p. 545.
[207] Cf. *Ibidem*.

sociedade democrática."[208]. Em termos simples, é através deste princípio que se materializa a ponderação de valores e interesses em conflito.

Assim, o legítimo sacrifício dos direitos fundamentais acima citados, em função da realização da justiça e da segurança dos cidadãos, deverá ser encontrado com recurso a critérios de proporcionalidade. Em primeiro lugar, pelo legislador, na configuração dos pressupostos de admissão do uso de *malware* e, depois, pelo aplicador na sua atividade de investigação criminal. Ou seja, este princípio deverá observar-se em dois níveis: primeiramente, na estruturação do regime jurídico do *malware*; depois, na sua concreta aplicação ao caso.

Em termos mais práticos, por exemplo, significa que o catálogo de crimes deverá ser preenchido por crimes graves, devido à gravidade do próprio meio de obtenção de prova[209] ou, por outras palavras, se quisermos, os crimes que legitimam este método têm de estar aptos a desencadeá-lo. Nunca devemos esquecer que, na segunda ponderação, é essencial para a legitimidade deste método haver factos concretos da prática do crime do catálogo, bem como a necessidade de recurso a este meio.

Em síntese, este princípio proíbe que a restrição vá mais além do que o necessário, para atingir um fim constitucionalmente legítimo[210].

Embora a ideia de proporcionalidade induza imediatamente ao âmbito da proibição de um regime excessivo, este princípio desdobra-se ainda em três vertentes fundamentais: adequação; necessidade; e proporcionalidade em sentido estrito[211].

4.5.1.2.1 Princípio da adequação ou idoneidade

Pressuposta a legitimidade do fim consignado na norma[212], importa verificar-se o princípio da adequação ou também designado da idoneidade.

Este princípio ilustra a relação de idoneidade que deve existir entre o meio oculto a utilizar e o fim que o mesmo se propõe alcançar, através de uma regulamentação parametrizante, fim que legitimamente se considera pertinente. O

---

[208] Cf. JORGE MIRANDA, *Manual de Direito Constitucional. Direitos fundamentais*, tomo IV, 5.ª edição, Coimbra, Coimbra Editora (Wolters Kluwer), 2012, p. 303.
[209] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 114.
[210] Cf. JORGE REIS NOVAIS, *As restrições aos Direitos*…, op. cit. (2.ª edição), p. 741.
[211] Cf. JORGE BACELAR GOUVEIA, *Manual de Direito Constitucional. II – Direito Constitucional Português*, 6.ª edição revista e atualizada, Coimbra, Almedina, 2016, p. 825.
[212] JORGE MIRANDA, *Manual de Direito Constitucional*, op. cit., p. 308.

método é adequado, se se apresentar apto à obtenção do resultado que lhe foi normativamente destinado [213].

Portanto, o princípio da adequação exige que os meios ocultos restritivos legalmente previstos sejam adequados para a prossecução dos fins visados, isto é, para salvaguarda de outros direitos ou interesses constitucionalmente garantidos. No nosso caso, o *malware* é idóneo por ser útil para a consecução das já referidas finalidades e permitir a aproximação do resultado pretendido[214].

Todavia, neste jogo de valores, há ainda que considerar se o poder público dispõe de meios menos restritivos e capazes de proporcionar o mesmo grau de realização do fim proposto[215].

4.5.1.2.2 Princípio da necessidade ou da exigibilidade

O princípio da necessidade, da exigibilidade ou da indispensabilidade mostra como, perante o meio oculto julgado adequado, se impõe fazer um juízo a respeito da sua indispensabilidade no leque de métodos de obtenção de prova que, do mesmo modo, sejam equivalentemente considerados aptos à obtenção do resultado pretendido[216]. Ou seja, o recurso ao *malware* será necessário sempre que não haja outro meio de obtenção de prova menos gravoso, do ponto de vista da respetiva lesão.

Posto isto, na construção do regime jurídico do *malware* deverá estar expresso que este método só poderá ser escolhido quando for efetivamente necessário e indispensável ao fim visado. Deste modo, garante-se que o juiz faça uma reflexão no sentido de verificar se entre os meios suscetíveis de serem utilizados, não existe um menos gravoso que possa obter o mesmo resultado[217].

Por sua vez, como refere DAVID SILVA RAMALHO, o que deve estar presente na lei é: a necessidade material, enquanto menor ingerência possível nos direitos fundamentais afetados; a necessidade espacial, no sentido de redução do âmbito

---

[213] Cf. JORGE BACELAR GOUVEIA, *Manual de Direito Constitucional*, op. cit., p. 825.
[214] Cf. JORGE REIS NOVAIS, *As restrições aos Direitos*…, op. cit. (2.ª edição), pp. 736-737. Igualmente relevante para esta questão, é o raciocínio apresentado por MARIA ANA BARROSO DE MOURA DA SILVEIRA, *Da Problemática da Investigação Criminal em Ambiente Digital – em Especial, sobre a Possibilidade de Utilização de Malware como Meio Oculto de Obtenção de Prova*, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Dissertação de Mestrado, Lisboa, Universidade Católica Portuguesa, Faculdade de Direito – Escola de Lisboa, 2016, pp. 34-36 (policopiada).
[215] Cf. JORGE REIS NOVAIS, *Os Princípios Constitucionais Estruturantes da República Portuguesa*, Coimbra, Coimbra Editora, 2011, p. 167.
[216] Cf. JORGE BACELAR GOUVEIA, *Manual de Direito Constitucional*, op. cit., pp. 825-826, e JORGE MIRANDA, *Manual de Direito Constitucional*, op. cit., p. 308.
[217] Cf. JORGE REIS NOVAIS, *As restrições aos Direitos*…, op. cit. (2.ª edição), p. 741.

geográfico de aplicação do meio[218]; a necessidade temporal, isto é, a delimitação da duração deste meio; e a necessidade pessoal, ou seja, aplicar este método só às pessoas por ele visadas[219]. Por outras palavras, pretende-se que o regime jurídico demonstre que este método oculto só será utilizado em último recurso, durante o menor tempo possível e afete o mínimo de pessoas necessárias.

Em conclusão, este princípio impõe que se recorra, para atingir o fim pretendido, ao meio necessário, exigível ou indispensável, no sentido do ser o mais suave para atingir o fim previsto[220].

4.5.1.2.3 Princípio da proporcionalidade *stricto sensu*

Embora o princípio da proporcionalidade em sentido estrito esteja diretamente relacionado com o princípio da necessidade, este significa que os meios legais restritivos e os fins obtidos devem situar-se numa justa medida[221], impedindo a adoção de meios legais restritivos, desproporcionados e excessivos em relação aos fins a conseguir. Trata-se de avaliar a relação entre o bem que se pretende prosseguir com a restrição e o bem fundamental protegido que resulta, naturalmente, afetado[222].

Ora, este meio encoberto é proporcional, se os efeitos escolhidos se apresentarem equilibrados dentro do tipo de meio considerado adequado e necessário, em concordância com a avaliação entre os custos a suportar e os benefícios a atingir[223].

No nosso caso, significa que o regime jurídico do *malware* deverá observar critérios de objetividade, para compensar a própria subjetividade prática no momento de decidir pelo emprego ou não deste método. Assim, estes critérios devem traduzir-se na gravidade do crime, nos indícios, na sanção previsível, nos indivíduos afetados e na essencialidade do meio para a prova do facto sob investigação.

---

[218] No nosso caso, esta questão não se aplica.
[219] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 205.
[220] Cf. JORGE REIS NOVAIS, *As restrições aos Direitos*…, op. cit. (2.ª edição), p. 741. Sobre a aplicação deste princípio ao uso de *malware*, ver MARIA ANA BARROSO DE MOURA DA SILVEIRA, *Da Problemática da Investigação Criminal em Ambiente*…, op. cit., pp. 36-41.
[221] Cf. JORGE MIRANDA, *Manual de Direito Constitucional*, op. cit., p. 308.
[222] Raciocínio também interessante quanto a este princípio é o de MARIA ANA BARROSO DE MOURA DA SILVEIRA, *Da Problemática da Investigação Criminal em Ambiente*…, op. cit., pp. 41-45.
[223] Cf. JORGE BACELAR GOUVEIA, *Manual de Direito Constitucional*, op. cit., p. 826.

Em suma, na prática, haverá arbítrio sempre que não for respeitado o princípio da adequação. Haverá excesso, se não se verificarem os princípios da necessidade e da proporcionalidade, em sentido estrito[224].

4.5.1.3 Princípio da subsidiariedade

Para além de se exigir a reserva de lei, nos âmbitos que acabámos de referir, na aplicação do método oculto deverá ter-se em consideração o princípio da subsidiariedade. Este está intimamente relacionado com o princípio da proporcionalidade, designadamente, no seu subprincípio da necessidade.

Na prática, este transpõe-se no uso de *malware* apenas e tão-só quando os meios 'descobertos' existentes não sejam aptos a satisfazer os interesses da investigação ou, quando de entre os meios ocultos, não exista um menos lesivo para satisfazer esses mesmos interesses. Como refere MANUEL DA COSTA ANDRADE, não basta que sem o *malware* a investigação se torne mais difícil; é necessário que se torne consideravelmente impossível.

4.5.1.4 Princípio da reserva do juiz

Na concretização prática da ponderação, é muito importante o princípio da reserva do juiz[225]. Este é o elemento concretizador e agregador dos postulados já analisados. Significa isto que uma norma aceitadora do uso de *malware* deverá atribuir ao juiz de instrução o poder de aferir o cumprimento dos pressupostos legais para a sua utilização. Ou seja, apesar de ao legislador caber o papel de uma ponderação prévia, aquando da redação da norma, é ao juiz de instrução que cabe analisar objetivamente os bens jurídicos em conflito, nos termos da lei e da CRP, decidindo, no caso em concreto, pela autorização ou não do recurso ao *malware*.

Este princípio obriga a que o juiz não se limite a aderir aos fundamentos do Ministério Público. Pelo contrário, deverá fundamentar a autorização, enunciando todos os elementos necessários para a diligência e, de forma autónoma, inteirar-se das circunstâncias de facto e de direito relevantes para a sua decisão[226].

---

[224] Cf. JORGE MIRANDA, op. cit., p. 308.
[225] Devido ao interesse para esta matéria, veja-se MARIA DE FÁTIMA MATA-MOUROS, *Juiz das Liberdades*…, op. cit..
[226] Cf. MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação…», op. cit., p. 550.

Por sua vez, o princípio da reserva do juiz também é essencial, pois, através dele, posteriormente, o visado tem a oportunidade de verificar se o método foi legítimo, bem como a validade da prova através dele obtida.

Em síntese, ao contrário do que tem vindo a acontecer noutros meios de obtenção de prova, o regime jurídico do *malware* não pode permitir o desvalorizar do papel do juiz de instrução. Ele é essencial face ao próprio dano que este meio reveste e garante a tutela dos direitos fundamentais. Não esquecer, ainda, que ele compensa e cura o visado, dado este tomar conhecimento da medida apenas e somente depois de ter sido 'prejudicado' por ela[227].

4.5.1.5 Respeito pelo núcleo essencial da vida privada

Não obstante o acima referido, importa salientar que serão sempre nulas as provas obtidas mediante intromissão abusiva na vida privada. Pois, neste caso, o legislador constituinte fez já a sua opção baseada na ponderação de interesses de sentido diferente.

Quer isto dizer que, embora os interesses em causa sejam os mesmos, isto é, da prevenção e da punição dos que atentem contra valores dignos de proteção penal, neste caso, a Constituição dá prevalência absoluta, definitiva e incondicionada ao direito à privacidade e à dignidade da pessoa humana. O legislador preferiu que alguns criminosos permaneçam impunes, mesmo quando haja absoluta certeza da sua responsabilidade na prática de um crime, a que algum inocente seja condenado com o efeito dos eventuais abusos que uma norma mais maleável pudesse induzir. Por esse motivo, será perpetuamente nula a prova incriminadora que seja obtida mediante abusiva intromissão na vida privada[228].

Em conclusão, para que o uso de *malware* seja legítimo como meio de obtenção de prova, é necessário estar previsto na lei, evitando o abuso, o arbítrio ou o excesso. Significa que deverá definir: em que casos o *malware* pode ser utilizado (catálogo de crimes); quem o pode autorizar (competência objetiva); durante quanto tempo (critério temporal); sobre que sujeitos (competência subjetiva); e qual o procedimento. Ou seja, no entendimento da jurisprudência do Tribunal Constitucional Federal Alemão, o

---

[227] Cf. MANUEL DA COSTA ANDRADE, op. cit., pp. 547-549, e ID., *"Bruscamente no Verão Passado"* …, op. cit., pp. 117-118.
[228] Cf. JORGE REIS NOVAIS, *As restrições aos Direitos*…, op. cit. (2.ª edição), pp. 578 e 580.

regime jurídico do *malware* deverá ser denso, claro e determinável, prevendo o fundamento, o fim e os limites da intromissão.

Por conseguinte, o aplicador da lei deverá efetuar uma segunda ponderação das condições da sua prática numa análise de proporcionalidade casuística. Perante uma panóplia de meios restritivos, deverá verificar se aquele meio é adequado no caso em questão. Entre os meios idóneos suscetíveis de serem utilizados em abstrato, deverá ser escolhido aquele que no concreto, face aos pressupostos da lei e às circunstâncias, se mostre necessário, exigível ou indispensável para atingir o fim pretendido[229]. Isto é, somente se poderá recorrer ao *malware* se nenhum outro meio idóneo, em primeira linha 'descoberto' e depois oculto, puder alcançar o mesmo resultado com um menor grau de lesão para a pessoa atingida. Por seu turno, para se recorrer a este método, não basta a suspeita, em concreto, da prática de um dos crimes previstos.

Finalmente, é muito importante não esquecer que a legitimidade do uso de *malware* passa por integrar soluções normativas indispensáveis à garantia da salvaguarda e inviolabilidade da área nuclear da intimidade. Esta salvaguarda far-se-á no momento em que se examinam e apreciam os dados recolhidos através do *malware*. No caso de se verificar a existência de dados que violam esta área nuclear, os mesmos deverão ser imediatamente destruídos[230].

[229] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 204.
[230] Cf. MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., pp. 116-117.

5. Outros meios ocultos

Como anotou MANUEL DA COSTA ANDRADE[231], o nosso ordenamento jurídico, ao contrário do alemão, carece de um regime geral de métodos ocultos de investigação criminal. Na verdade, o que existe são sucessivos diplomas, sem qualquer sistematização formal ou de ordem valorativa, nomeadamente o CPP, a Lei n.º 101/2001, de 25 de agosto (doravante designada por Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal), a Lei n.º 5/2002, de 11 de janeiro[232], e a LC. Dito de outro modo, e socorrendo-nos da opinião expressa por DAVID SILVA RAMALHO, acerca desta matéria, não raras vezes estamos perante "*verdadeiras ilhas processuais de exceção ao regime geral, sem uma consagração estável dos pressupostos que permitem a navegação para as mesmas ou de umas para as outras*"[233].

Não obstante, do conjunto diversificado e heterogéneo de meios ocultos existentes, que permitem à entidade que investiga intrometer-se na esfera privada das pessoas investigadas, é possível encontrar, como demonstraremos, uma unidade comum de requisitos e exigências para que seja autorizada a sua utilização, e fora dos quais a mesma é considerada abusiva.

Assim, no presente capítulo, o que nos propomos analisar é o regime jurídico das escutas telefónicas e das ações encobertas, de modo a aferir quais os requisitos materiais e formais comuns relevantes para um qualquer regime jurídico de meios ocultos.

Decidimos analisar especificamente estes dois regimes porque, por um lado, as escutas telefónicas são consideradas a primeira forma oculta de investigação[234], que abriu portas a outros meios encobertos, e o seu regime jurídico foi ao longo dos anos modelado pelo legislador, pela doutrina e pela jurisprudência. Deste modo, em teoria, possuímos a maturidade jurídica necessária para chegarmos a conclusões seguras sobre os requisitos obrigatórios para a regulamentação do regime jurídico do *malware*. Por outro lado, as ações encobertas são consideradas o segundo meio oculto relevante[235], e

---

[231] Cf., deste autor, «Métodos ocultos de investigação…», op. cit., pp. 539-540.
[232] Diploma que estabelece medidas de combate à criminalidade organizada e económico-financeira.
[233] Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 185.
[234] Cf. MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação…», op. cit., p. 532.
[235] Cf. *Ibidem*, p. 534.

entendemos que, ao nível da danosidade, aproxima-se muito ao *malware*[236], sem deixar de esquecer que há quem considere este meio regulado pelo n.º 2 do artigo 19.º da LC.

Em síntese, o que pretendemos é identificar as coordenadas e os princípios para os utilizar na construção do regime jurídico para o *malware*. Não pretendemos, pois, proceder ao exercício do início de uma teoria geral dos meios ocultos de investigação, mas antes proceder a um adequado levantamento.

5.1 Escutas telefónicas

No presente subtítulo, intentamos abordar, ainda que de forma genérica, os requisitos necessários para que uma escuta seja autorizada. Não procedemos a uma análise detalhada sobre este meio de obtenção de prova, mas apenas elencamos os pressupostos para a sua utilização.

Em torno deste regime estão relacionadas questões como: as conversas entre o arguido e o seu defensor; conversações cobertas pelo segredo profissional, de funcionário ou de Estado; transcrições; conhecimentos fortuitos; e efeito à distância. Todavia, por não se relacionarem diretamente com o que pretendemos demonstrar, não as abordaremos.

As escutas telefónicas, como meio de obtenção de prova, previsto e regulado nos artigos 187.º e seguintes do CPP, revestem-se, como refere MANUEL DA COSTA ANDRADE[237], de uma danosidade polimórfica. De um lado, estamos perante um meio lesivo do direito à palavra, à privacidade ou à intimidade; do outro, diante de uma violação do direito do arguido a não contribuir positivamente para a sua condenação[238]. Todavia, no outro prato da balança, estão valores como a necessidade de realização da justiça e da descoberta da verdade material.

Assim, e nos termos do n.º 2 do artigo 18.º da CRP, foi erigido um regime que prevê a utilização desta técnica para obtenção de prova, o qual tem subjacente a ponderação de valores e interesses realizada pelo legislador, nomeadamente, com

---

[236] Segundo RITA CASTANHEIRA NEVES, *As Ingerências nas Comunicações*…, op. cit., p. 281, as ações encobertas constituem possivelmente o meio de obtenção de prova mais lesivo, dentre os que se encontram consagrados no nosso ordenamento jurídico.
[237] Cf. MANUEL DA COSTA ANDRADE, «Das Escutas Telefónicas», *in* Manuel Monteiro Guedes Valente (coord.), *I Congresso de Processo Penal*, Coimbra, Almedina, 2005, p. 216.
[238] Cf. *Ibidem*, pp. 216-217.

respeito pelos princípios da proporcionalidade, da adequação e da necessidade, referidos no supracitado artigo[239].

As escutas telefónicas são, assim, uma restrição admitida pelo legislador constitucional em matéria de processo penal, nomeadamente nos termos do n.º 4 do artigo 34.º da CRP. Deste modo, contraria-se a proibição que resulta do n.º 8 do artigo 32.º da CRP e do n.º 3 do artigo 126.º da CPP, os quais consideram nulas todas as provas obtidas mediante abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações.

Em conclusão, o regime legal que está consagrado atualmente é o que corresponde à ponderação de interesses desejado pelo legislador[240], estando o mesmo estruturado de forma a existir uma adequada proteção dos direitos fundamentais.

Contudo, além desta ponderação, cabe ao juiz de instrução criminal efetuar, no caso concreto, uma segunda reflexão.

Nesse sentido, consagra a letra da lei os seguintes critérios materiais de admissibilidade da escuta telefónica: ser "*indispensável para a descoberta da verdade*" ou ser a prova *"de outra forma, impossível de obter*". Quer isto dizer que o legislador procurou salientar a excecionalidade e a proporcionalidade que deverá revestir o recurso a este meio.

Entende JOSÉ MANUEL DAMIÃO DA CUNHA que "*existe uma clara intenção de afirmar, e acentuar, a "excepcionalidade" (quando não o carácter de ultima ratio) do recurso às escutas telefónicas."*[241]. No mesmo sentido, CARLOS ADÉRITO TEIXEIRA defende que "*não há dúvida de que o legislador no n.º 1 do art. 187.º do CPP procurou reforçar o carácter excepcional e subsidiário deste meio de obtenção de prova, num quadro de aplicação restritiva, decalcada num grau de exigência elevado assente na indispensabilidade para a "descoberta da verdade" ora na impossibilidade ou particular dificuldade para obter "prova" por outra via."*[242].

Relativamente à subsidiariedade, impôs o legislador que só é possível recorrer a este mecanismo quando, de outra forma, não for possível ou for muito difícil obter

---

[239] Cf. Acórdão do Tribunal da Relação de Lisboa, de 10-05-2011 (Margarida Blasco), processo n.º 65/11.0JAFUN-A.L1-5, disponível em http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/a4c72ca6744d803f802578a80051d2a1?OpenDocument [consultado a 09-12-2017].

[240] Cf. MANUEL DA COSTA ANDRADE, «Das Escutas Telefónicas», op. cit., p. 217.

[241] Cf. JOSÉ MANUEL DAMIÃO DA CUNHA, «O Regime Legal das Escutas Telefónicas – Algumas Breves Reflexões», *Revista do CEJ*, número 9 (especial), 1.º semestre de 2008, p. 207.

[242] Cf. CARLOS ADÉRITO TEIXEIRA, «Escutas Telefónicas: A Mudança de Paradigma e os Velhos e os Novos Problemas», *Revista do CEJ*, número 9 (especial), 1.º semestre de 2008, p. 243.

prova. Significa isto que, na autorização da escuta, deverá haver um reforço da ponderação dos princípios da adequação e da necessidade.

Além destes critérios essenciais, também deverá ser observado: (1) a fase do processo; (2) a competência para a autorização; (3) o catálogo de crimes; (4) o catálogo de sujeitos; (5) o prazo de autorização; e (6) o procedimento previsto no artigo 188.º do CPP.

5.1.1 Fase do processo e competência

Hoje em dia, e caso se cumpra escrupulosamente a lei, só poderá ser autorizada uma escuta telefónica em situações de crimes já cometidos ou iniciados, pelo que a mesma não é admissível com a finalidade de prevenção criminal. Está, assim, dependente da abertura do inquérito, ou seja, não poderá ser autorizada e realizada numa outra fase processual.

Relativamente à competência, só o juiz de instrução poderá determinar a escuta telefónica, mas mediante requerimento do Ministério Público.

Em consequência, deverá ter-se em atenção os dois critérios acima mencionados: a indispensabilidade para a descoberta da verdade; ou o juízo sobre a impossibilidade ou grande dificuldade para obter a prova. Na ponderação dos mesmos, é necessário ter uma noção precisa de qual a verdade material que se pretende obter ou, então, um juízo de valor sobre os meios de obtenção de prova alternativos. É precisamente aqui que surgem as principais dificuldades.

Por um lado, impôs-se uma delimitação dos factos a investigar que, geralmente, ainda não se encontram presentes no momento que se requer a escuta. Por outras palavras, o juiz de instrução criminal tem de efetuar uma ponderação baseada em hipóteses ou probabilidades dos elementos de prova que se poderiam obter com recurso à escuta telefónica, e que não seriam possíveis de obter através de outros meios menos lesivos[243].

Além disso, nesta fase, não se tem ainda a noção exata da respetiva configuração, porque não foram produzidos outros meios de prova alternativos[244]. Se já

[243] Cf. ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., p. 790.

[244] Considera o Acórdão do Tribunal da Relação de Évora, de 17-03-2015 (Martins Simão), processo n.º 55/11.2GDSTC.E1, que "é *possível lançar-se mão das escutas telefónicas logo como o primeiro meio de obtenção da prova utilizado, quando – e apenas nesta hipótese – o juiz de instrução se convença, em face dos concretos dados factuais trazidos pelo Ministério Público, que ela é a única diligência capaz de fazer*

o tivessem sido, perdia-se todo o interesse na escuta como meio oculto, uma vez que o(s) arguido(s) já estaria(m) desperto(s) para esta possibilidade[245].

Em suma, e como salienta MARIA DE FÁTIMA MATA-MOUROS[246], é muito difícil decidir sobre a autorização deste meio encoberto, dado que na altura de o fazer falta a orientação da lei e tanto um como outro critério sofrem de uma indeterminação concetual.

A este propósito, já a doutrina alemã (antes da nossa reforma do CPP, em 2007) tinha identificado a existência de uma "*inexequibilidade da cláusula de subsidiariedade nas normas habilitantes das medidas para além das dificuldades praticamente inultrapassáveis na aplicação rigorosa do princípio da proporcionalidade. É que não sendo viável uma graduação em abstrato das medidas de investigação em função de critérios como o da respetiva potencialidade lesiva para os direitos dos visados ou do grau de eficiência que oferecem para a investigação de cada tipo de crime, dificilmente a cláusula da subsidiariedade poderá adquirir eficácia prática*."[247].

No que diz respeito ao pedido, o juiz não poderá determinar a escuta para além do que é requerido pelo Ministério Público. Por exemplo, não deverá autorizar a escuta a pessoa ou telefone diverso ou por prazo superior ao requerido. Contudo, pode ficar aquém, isto é indeferir a escuta de certas pessoas ou telefones, ou deferir por um prazo inferior ao solicitado[248].

Quanto à decisão judicial, deverá ser fundamentada, demonstrando as razões que face ao artigo 187.º do CPP levam o juiz a autorizar este meio oculto. Segundo PAULO PINTO DE ALBUQUERQUE[249], a decisão poderá ser fundamentada na promoção do Ministério Público sobre que incidiu, dando por reproduzidos os fundamentos da mesma.

---

carrear para os autos os elementos probatórios aptos à descoberta da verdade." Ver Acórdão disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/6a827b6477ada98880257e20003c4c74?OpenDocument [consultado a 12-12-2017].

[245] Cf. ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., p. 790.

[246] Cf. MARIA DE FÁTIMA MATA-MOUROS, «Escutas Telefónicas – O que não Muda com a Reforma», *Revista do CEJ*, número 9 (especial), 1.º semestre de 2008, p. 239.

[247] Cf. *Ibidem*, pp. 240-241.

[248] Cf. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2.ª edição, Lisboa, Universidade Católica Editora, 2008, p. 508.

[249] Cf. *Ibidem*.

Na decisão judicial, a exigência de indicação dos factos[250], em relação aos quais se autoriza a escuta, não constitui uma formalidade essencial, em virtude de aquilo que está em causa serem crimes e não factos[251]. Isto porque o juiz não dispõe de uma 'bola de cristal' para poder, antes da realização da escuta, contemplar sobre quais os factos que este meio de investigação irá incidir[252].

Também não é exigível ao juiz fundamentar a decisão com a exclusão de outros meios de obtenção de prova, demonstrando o porquê de ser impossível ou muito difícil obter prova sem o recurso às escutas telefónicas. Com efeito, "*para afirmarmos que os outros meios não servem para o caso concreto temos de nos firmar numa conjectura sobre o seu valor pois que não foram produzidos*" e se o fossem já teriam colocado o(s) arguido(s) em alerta[253].

5.1.2 Catálogo de crimes

É o próprio artigo 187.º do CPP que estabelece o catálogo de crimes. Dentre eles, constam: os puníveis com pena de prisão superior, no seu máximo, a 3 anos; os relativos ao tráfico de estupefacientes e armas; o terrorismo, a criminalidade violenta ou altamente organizada; o sequestro, rapto ou tomada de reféns; ou, ainda, os crimes contra a segurança do Estado.

Só no caso de estarmos perante um crime desse conjunto, será possível autorizar a escuta; caso contrário, o meio de obtenção de prova deverá ser indeferido[254]. O intuito foi precisamente de limitar o âmbito de aplicação deste meio encoberto a qualquer

---

[250] Cf. Acórdão do Supremo Tribunal de Justiça, de 26-03-2014 (Santos Cabral), processo n.º 15/10.0JAGRD.E2.S1, disponível em http://www.dgsi.pt/jstj.nsf/-/C48079CB0B1E7B0180257CF2005184CA [consultado a 12-12-2017].

[251] Cf. ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., p. 791. Neste ponto, e utilizando o raciocínio elaborado por MARIA FERNANDA PALMA, a propósito da teoria do crime na investigação criminal, entendemos que o juiz deverá ter em consideração a mera probabilidade de se puderem vir a confirmar factos com características de crime. Cf. «A teoria do crime como teoria da decisão penal e o Direito da Investigação Criminal», *in Direito da Investigação Criminal e da Prova*, coord. Maria Fernanda Palma *et al*., Coimbra, Almedina, 2014, p. 22.

[252] Em sentido contrário, ver ANA RAQUEL CONCEIÇÃO, *Escutas Telefónicas*, Lisboa, Quid Juris, 2009, pp. 105 e ss., citado por ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., p. 791.

[253] Cf. ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., p. 792.

[254] Cf. Acórdão do Tribunal da Relação de Coimbra, de 06-04-2011 (Orlando Gonçalves), processo n.º 111/10.4JALRA-A.C1, disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/bd76f98b662ab9ac8025787100514ad9?OpenDocument [consultado a 10-12-2017].

crime, isto é, nas palavras de MANUEL DA COSTA ANDRADE[255], de não fazer com uma bomba atómica o que se pode fazer como uma carabina.

Acresce, ainda, que deve existir uma suspeita fundada (e não uma mera suspeita) da prática de um crime do catálogo. Dito de outro modo, deve existir um certo nível de indícios, ou seja, a autorização deve ser fundada em factos determinados como diz a lei, não bastando a notícia do crime ou a denúncia[256].

Conclui-se, assim, que o juiz tem de verificar, aquando da autorização, se existem indícios da prática de um crime[257] que permitem o recurso a este meio de investigação, devendo discriminar o(s) mesmo(s) e os elementos probatórios.

5.1.3 Catálogo de sujeitos

O artigo 187.º do CPP definiu também o universo de potenciais destinatários da escuta, ou seja, as pessoas contra quem este meio pode incidir. Como catálogo de sujeitos, podemos elencar: o arguido ou o suspeito; o intermediário; e a vítima.

O objetivo da existência de um catálogo fechado de sujeitos é obstar a que possam existir escutas contra incertos, porquanto as mesmas só poderão recair sobre pessoas concretas[258]. No entanto, não quer isto dizer que será sempre necessário conhecer a identidade civil da pessoa sob escuta, apenas se exige que a mesma seja uma pessoa concreta e determinada[259].

É considerado suspeito, nos termos da alínea e) do artigo 1.º do CPP, "*toda a pessoa relativamente à qual exista indício de que cometeu ou se prepara para cometer um crime, ou que nele participou ou se prepara para participar*". Como refere INÊS FERREIRA LEITE[260], basta que hajam indícios de que tal pessoa seja suspeita e que

---

[255] Cf. MANUEL DA COSTA ANDRADE, «Das Escutas Telefónicas», op. cit., p. 218.

[256] Ver Acórdão do Tribunal da Relação de Lisboa, de 10-05-2011 (Margarida Blasco), processo n.º 65/11.0JAFUN-A.L1-5.

[257] Como refere MARIA FERNANDA PALMA, «A teoria do crime…», op. cit., pp. 20-21, na investigação criminal é muito importante trabalhar-se com a ideia de crime e, em concreto, com a hipótese de determinados factos poderem vir a ser qualificados como crimes. A conclusão do juiz de que certo facto é crime pressupõe uma operação na qual se comparam as características de um facto em concreto com as do tipo legal.

[258] Cf. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), p. 509.

[259] A este propósito, consultar o Acórdão do Tribunal da Relação do Porto, de 11-02-2015 (Neto de Moura), processo n.º 2063/14.2JAPRT-A.P1, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/f2cd9bcbafe3b34080257df7004ca094?OpenDocument [consultado a 10-12-2017].

[260] Ver «O novo regime das escutas telefónicas. Uma visão panorâmica sobre a reforma de 2007», *in Direito da Investigação Criminal e da Prova*, coord. Maria Fernanda Palma *et al*., Coimbra, Almedina, 2014, p. 262.

esses indícios apontem para um concreto aparelho que permita a sua posterior identificação.

Aquando do pedido de autorização da escuta telefónica deverá ser especificado o(s) número(s) de telefone ou telemóvel que se pretende(m) intercetar, independentemente de a propriedade ser do suspeito ou do arguido.

Em relação aos telemóveis, existe doutrina que tem vindo a discutir se a escuta deverá ser autorizada em relação ao número do telefone ou em função do IMEI. Segundo PAULO PINTO DE ALBUQUERQUE, "*a escuta só deve ser autorizada em relação ao número atribuído ao arguido ou ao suspeito, negando-se a escuta a sucessivos cartões que no mesmo [telemóvel] venham a ser introduzidos, bem como os sucessivos aparelhos que venham a albergar esses cartões*"[261]. Não obstante, há também quem considere[262] que cada situação deverá ser devidamente ponderada, podendo aceitar-se que a escuta verse sobre o telefone que é utilizado, desde que para o efeito haja a notícia de que o sujeito utiliza diversos cartões, isto porque, frequentemente, os agentes dos crimes munem-se de vários artifícios para fugir às malhas da lei.

Relativamente ao intermediário, podemos considerar toda aquela pessoa que pela sua proximidade com o arguido ou suspeito, seja por ser familiar ou amigo, ou por outras razões que levem ao contacto entre ambos, ainda que ocasionalmente ou forçado, se configure como potencial interlocutor. Ademais, por qualquer uma das formas previstas nos artigos 187.º e 189.º do CPP, sobre quem, pela respetiva autoridade judiciária, recaiam suspeitas fundadas de, nos referidos contactos, serem discutidos assuntos que, direta ou indiretamente, se prendem com o crime em investigação[263].

Este intermediário, segundo CARLOS ADÉRITO TEIXEIRA[264], pode ser imediato ou mediato, desde que se mantenha a exigência de a informação se destinar ou ser proveniente do arguido ou do suspeito. A este propósito, PAULO PINTO DE

---

[261] Cf. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), p. 509.
[262] Neste sentido, ver ANTÓNIO DA SILVA HENRIQUES GASPAR *et al.*, *Código de Processo Penal Comentado*, op. cit., p. 794.
[263] Cf. Acórdão do Tribunal da Relação de Lisboa, de 06-12-2007 (Almeida Cabral), processo n.º 10278/07-9, disponível em http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/4dc6137fc33fb088802573aa005535bb?OpenDocument [consultado a 09-12-2017].
[264] Cf. CARLOS ADÉRITO TEIXEIRA, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., p. 250.

ALBUQUERQUE[265] acrescenta que não é necessário verificar a má-fé ou o dolo do mesmo, bastando que seja um "participante necessário" naquela conversa.

Por fim, quanto às vítimas do crime "*poderão ser os titulares do bem jurídico que têm a faculdade de se constituírem como assistentes, mas também os titulares de um bem jurídico que seja, de modo mediato ou difuso, tutelado pelo tipo, quando se trate de um crime de perigo ou que tutele uma multiplicidade de bens*"[266]. A escuta só poderá ser realizada mediante consentimento expresso ou presumido caso a vítima esteja incontactável. Porém, a vítima, como sujeito da escuta, só tem interesse para a investigação relativamente a um pequeno leque de crimes.

Quanto à competência para a sua qualificação, caberá ao Ministério Público definir quem considera suspeito ou arguido no requerimento de realização da escuta. Por sua vez, o juiz de instrução criminal só poderá contestar essa qualificação se for manifestamente ilegal. Relativamente ao intermediário, como cabe ao Ministério Público ser o *domnus* do inquérito, também cabe a ele determinar se uma concreta pessoa atua como tal, podendo o juiz de instrução criminal controlar a legalidade após tomar conhecimento da escuta. Por fim, quanto à vítima, o Ministério Público deve juntar o seu consentimento e indicar as razões de facto e de direito pelas quais considera tratar-se como tal, podendo, por seu turno, o juiz de instrução fazer uma apreciação de mérito[267].

Não podemos deixar de referir, ainda que a título indicativo, que são expressamente proibidas as escutas entre o arguido e o seu defensor (n.º 5 do artigo 187.º do CPP), bem como entre as pessoas com legitimidade para recusar o depoimento em nome do segredo profissional (alínea b do n.º 6 do artigo 188.º do CPP), exceto nos casos previstos na lei. Opostamente, as escutas podem ser efetuadas contra pessoas que têm o direito de se recusar a depor como testemunhas, nos termos do artigo 134.º do CPP. Se assim não fosse, este direito prevalecia sobre o interesse da investigação, impedindo a regular obtenção de prova ou descoberta da verdade material. Por último,

---

[265] Cf. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), p. 509.
[266] Cf. INÊS FERREIRA LEITE, «O novo regime das escutas telefónicas…», op. cit., p. 263.
[267] Cf. *Ibidem*, pp. 263-264.

estamos perante circunstâncias distintas – a escuta e o depoimento –, tratando-se de processos autónomos[268].

Acresce referir que é indiferente o local onde se encontra o sujeito da escuta, quando a mesma é realizada. Importa antes que o telemóvel integre a rede nacional de telecomunicações, isto é que a operadora seja portuguesa.

5.1.4 Prazo de autorização

Prevê o n.º 6 do artigo 187.º do CPP que "*a interceção e a gravação de conversações ou comunicações são autorizadas pelo prazo máximo de três meses, renovável por períodos sujeitos ao mesmo limite, desde que se verifiquem os respetivos requisitos de admissibilidade.*"[269]. A contagem deste prazo inicia-se à data da prolação do despacho judicial que autoriza a escuta, e não a partir do efetivo início da interceção[270].

A questão que ora se coloca é de saber qual o prazo de duração máxima da escuta. Há alguma doutrina[271] em defesa de que é o da duração do inquérito, não podendo a mesma ser renovada depois desse período, mas pode manter-se findo o inquérito. Em sentido contrário[272], há quem considere que ao atingir-se o prazo máximo, devem cessar todas as escutas em curso. Outra doutrina[273] é de opinião que o prazo da escuta é autónomo e distinto do prazo do inquérito previsto no artigo 276.º do CPP, motivo pelo qual este último poderá ser ultrapassado, nomeadamente por razões de complexidade do processo, enquanto a duração da escuta é determinado em virtude de

---

[268] Neste sentido, ver PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), pp. 510-511, e CARLOS ADÉRITO TEIXEIRA, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., p. 252.

[269] Cf. MARIA DE FÁTIMA MATA-MOUROS, «Escutas Telefónicas – O que…», op. cit., pp. 237-238, saúda a previsão de um limite máximo, contudo crítica o prazo adotado (3 meses). Refere que este prazo deveria ser reduzido, em virtude de existirem estudos, nomeadamente na Alemanha, que concluem que o juiz autoriza sempre a escuta pelo prazo máximo.

[270] Cf. Acórdão do Tribunal da Relação de Coimbra, de 19-02-2014 (Olga Maurício), processo n.º 528/07.1GCVIS.C1, disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/805204801df6667b80257c890034f437?OpenDocument [consultado a 10-12-2017].

[271] Ver por exemplo, NUNO SERRÃO DE FARIA, «Acesso ao registo das escutas telefónicas», *in* AA.VV., *Prova criminal e direito de defesa: estudos sobre teoria da prova e garantias de defesa em processo penal*, coord. Teresa Pizarro Beleza *et al*., Coimbra, Almedina, 2011, p. 210, citado por ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., p. 813.

[272] Cf. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), p. 511.

[273] Neste sentido, consultar ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., pp. 813-814.

já não se observarem os pressupostos que levaram à sua determinação. Ambos podem manter-se, ainda que por razões completamente distintas.

Quanto a esta questão, assumimos uma postura intermédia, mesclada no entendimento de NUNO SERRÃO DE FARIA e de PAULO PINTO DE ALBUQUERQUE, ou seja, de que o prazo máximo é o da duração do inquérito, podendo terminar a escuta em curso[274]. Caso assim não fosse, com a aproximação do termo do inquérito, não poderia ser renovado o prazo da escuta, se o mesmo viesse a terminar posteriormente à duração deste.

5.1.5 Procedimentos

Quanto às formalidades, encontram-se reguladas matérias relativas à "reserva do juiz", prevista no n.º 4 do artigo 32.º da CRP, e matérias referentes à conservação ou utilização da prova.

O juiz quando autoriza a escuta identifica o(s) sujeito(s) e fixa um prazo para a mesma, com o limite de três meses. No começo da interceção, o órgão de polícia criminal elabora um auto de início[275], onde constará: a menção do despacho de autorização; a identidade da pessoa que procede à diligência; a identificação do telefone em causa; e o circunstancialismo de tempo, modo e lugar da interceção.

Posto isto, a cada décimo quinto dia contado desde o início da interceção, o órgão de polícia criminal tem de elaborar um auto intercalar e um relatório.

O auto de interceção e gravação (que tem de obedecer ao disposto no artigo 99.º do CPP) deve indicar: a data e a hora de cada comunicação intercetada; a identificação do sujeito e das pessoas intervenientes na conversação; e da pessoa que procedeu à recolha deste elemento de prova.

O órgão de polícia criminal que efetuar a interceção deverá lavrar em auto o conteúdo das conversações e comunicações intercetadas e gravadas. Deverá elaborar ainda um relatório onde indique: as passagens das gravações relevantes para a prova; descrever, sucintamente, o respetivo conteúdo e explicar o alcance do mesmo para a descoberta da verdade material; indicar as passagens que poderão revestir interesse para efeitos de aplicação de meios de coação; e indicar as comunicações, relatórios e suportes técnicos que considere manifestamente estranhos ao processo.

---

[274] Aparentemente no mesmo sentido, ver INÊS FERREIRA LEITE, «O novo regime das escutas telefónicas…», op. cit., pp. 260-261.

[275] O qual deverá ser comunicado ao juiz de instrução criminal que autorizou a interceção, para que tenha conhecimento do início da escuta.

Os supracitados auto intercalar e o relatório são remetidos ao Ministério Público, para, no prazo de quarenta e oito horas[276], o mesmo avaliar e pronunciar-se sobre estes na sua promoção, apresentando, obrigatoriamente, o auto e o relatório ao juiz. Em consequência, este deve, o mais depressa possível, proferir despacho.

Nesse despacho, o juiz decide se se mantém a indispensabilidade da escuta ou não. Em caso afirmativo, determina a junção provisória aos autos dos suportes técnicos que acompanham o auto e o relatório, podendo ordenar que a escuta se mantenha pelo prazo fixado ou modificar o mesmo. Em caso negativo, pode ordenar que a escuta não se mantenha para determinados sujeitos. Não obstante, em nenhuma das hipóteses poderá pronunciar-se definitivamente sobre a validade da escuta.

Este despacho é provisório e objetiva garantir o controlo do juiz relativamente aos prazos, à autorização e prorrogação e comprovar a relevância dos elementos recolhidos.

Por último, não podemos deixar de referir que as pessoas escutadas podem examinar os respetivos suportes técnicos até ao encerramento da audiência, a fim de controlarem a legalidade e regularidade da transcrição, apresentar a sua defesa e contextualizar determinada passagem, entre outros motivos.

Salientamos que quanto ao procedimento, a doutrina[277] discute matérias como: a proximidade temporal do acompanhamento judicial; a desmaterialização desse acompanhamento; e a destruição de suportes técnicos e dos relatórios sem o exercício do contraditório. Uma vez que ultrapassam o objetivo do presente subtítulo, não nos debruçámos sobre elas.

5.1.6 Extensão

A questão agora em debate é a de averiguar a que realidades se deverá estender o regime das escutas telefónicas, nos termos do artigo 189.º do CPP.

Importa, antes de mais, salientar que alguma doutrina considera o artigo 189.º parcialmente revogado. Nesse sentido, PAULO DÁ MESQUITA e RITA

---

[276] Ainda quanto a esta matéria, há autores que discutem o modo de contagem deste prazo, nomeadamente se este terminar durante um dia não útil, à semelhança do que prevê o Código de Processo Civil, passará para o dia útil seguinte. Cf. CARLOS ADÉRITO TEIXEIRA, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., pp. 253-254.

[277] Sobre estas matérias, consultar: PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), pp. 514 e ss; ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., pp. 815 e ss; CARLOS ADÉRITO TEIXEIRA, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., pp. 253 e ss; e MARIA DE FÁTIMA MATA-MOUROS, «Escutas Telefónicas – O que…», op. cit., pp. 223 e ss.

CASTANHEIRA NEVES[278] entendem que o n.º 1 do artigo 189.º do CPP foi em parte substituído pela regulação mais completa e exaustiva da LC, na medida em que o seu artigo 18.º regula o recurso à interceção e registo de comunicações, e o n.º 4 refere que os regimes dos artigos 187.º, 188.º e 190.º do CPP apenas são aplicáveis "*em tudo o que não for contrariado pelo presente artigo*". Com o mesmo entendimento, JOÃO CONDE CORREIA[279] refere que "*parece hoje inquestionável que primeiro a Lei n.º 32/2008 e depois a Lei n.º 109/2008 revogaram, tacitamente, parcelas importantes do regime consagrado no artigo 189.º do Código de Processo Penal*."[280]. Assim, esta revogação, ainda que não expressamente, apresenta-se geradora de problemas ao nível da interpretação e da aplicação do direito constituído.

Em sentido contrário, PAULO PINTO DE ALBUQUERQUE[281] afirma que o artigo 18.º da LC não revogou o artigo 189.º do CPP.

Ora, independentemente dessas divergências, no presente subtítulo pretendemos apenas e a título meramente indicativo elencar quais as possíveis extensões do regime das escutas telefónicas, mas sem nunca deixar de alertar o leitor para a jurisprudência e doutrina que consideram que algumas delas já se encontram reguladas na LC.

Nas palavras de MANUEL DA COSTA ANDRADE[282], o artigo 189.º do CPP é uma verdadeira "casa de horrores" hermenêuticos, porque aplica ao regime da interceção das telecomunicações casos que reclamam tratamento diferenciado.

Segundo CARLOS ADÉRITO TEIXEIRA, pode entender-se que a extensão do artigo 189.º envolve cinco dimensões: "*i) do telefone a outros meios técnicos; ii) da voz humana à imagem; iii) da ingerência (no conteúdo das) nas conversações ou comunicações para obtenção do registo de realização das mesmas; v) e daquela ingerência "transambiental" para a localização geográfica do aparelho técnico da comunicação*" [283]. Encara ainda com naturalidade que o legislador previsse dentro deste

---

[278] Cf. PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, op. cit. pp. 102 e ss, e RITA CASTANHEIRA NEVES, *As Ingerências nas Comunicações*…, op. cit., pp. 280 e 285.
[279] Cf. JOÃO CONDE CORREIA, «Prova digital: as leis que temos e a lei que devíamos ter», op. cit., p. 36.
[280] Neste sentido, veja-se o Acórdão do Tribunal da Relação de Évora, de 20-01-2015 (João Gomes de Sousa), processo n.º 648/14.6GCFAR-A.E1, disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument [consultado a 16-12-2017].
[281] Cf. AA.VV., *Código de Processo Comentado*, Coimbra, Almedina, 2014, p. 837, citado por JOÃO CONDE CORREIA, «Prova digital: as leis que temos e a lei que devíamos ter», op. cit., p. 36.
[282] Ver *"Bruscamente no Verão Passado"* …, op. cit. p. 185.
[283] Cf. CARLOS ADÉRITO TEIXEIRA, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., p. 281.

regime outras possibilidades, nomeadamente as comunicações efetuadas por meio de um sistema informático. No entanto, alerta para o facto de que se deverá verificar se as especificidades técnicas dos outros meios de comunicação se devem inserir neste regime ou, pelo contrário, merecem um tratamento jurídico unitário e coerente.

5.1.6.1 Correio eletrónico

Com a redação do artigo 189.º, o legislador pretendeu estender o regime das escutas ao *e-mail*[284]. Fê-lo de forma direta, quando referiu "*designadamente correio eletrónico*". Para os casos de impossibilidade de interceção em tempo real, acrescentou "*mesmo que se encontrem guardados em suporte digital*"[285].

Embora o legislador pretendesse alargar o regime das escutas telefónicas às comunicações acabadas de ser rececionadas no correio eletrónico e às que já se encontram arquivadas noutra componente de *software* do equipamento, em verdade, estamos perante duas realidades distintas.

O correio eletrónico, depois de recebido, aberto e lido, continua a ter a mesma proteção que o correio fechado, isto é, acabado de ser rececionado. No entanto, o *e-mail* recebido, lido e guardado no computador do destinatário deveria deixar automaticamente de ser entendido como telecomunicação, passando a valer como um mero documento, sem necessidade de proteção adicional. Só a correspondência fechada, tem natureza sigilosa e deve gozar de proteção constitucional. No caso de *e-mail* já aberto e guardado no sistema informático, deveria ser-lhe aplicável o regime das buscas e apreensões[286].

Porém, a redação atual não faz esta distinção. Tanto num caso como noutro, devemos ter em atenção o catálogo taxativo de crimes, a intervenção do juiz de

---

[284] Os *e-mails* não necessitam apenas de conter 'palavras'; podem conter imagens ou vídeos. Estende-se o previsto também aos seus anexos.

[285] Segundo PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, op. cit., p. 90, esta é uma inovação que para além de ser infundada se apresenta como imprecisa, carecendo de explicitação de um critério delimitador entre âmbito de proteção das comunicações cobertas pela norma, essencial para identificar a autonomia de dados guardados que tenham sido transmitidos no passado.

[286] Como refere MANUEL DA COSTA ANDRADE, *"Bruscamente no Verão Passado"* …, op. cit., p. 185, "*por seu turno e porque (já) praticamente nada têm a ver com a intromissão nas telecomunicações, e praticamente tudo têm a ver com as buscas e as apreensões, deveriam reconduzir-se a estes regimes as intromissões nos documentos – e concretamente nas mensagens transmitidas por e.mail depois de recebidas, abertas e lidas – que o destinatário guarda no seu computador*". Ver também PEDRO VERDELHO, «Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital», *Revista do CEJ*, número 9 (especial), 1.º semestre de 2008, pp. 163-166, ANTÓNIO DA SILVA HENRIQUES GASPAR *et al.*, *Código de Processo Penal Comentado*, op. cit., pp. 835-836, e CARLOS ADÉRITO TEIXEIRA, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., pp. 281 e ss.

instrução e a observância dos trâmites do procedimento do artigo 188.º do CPP, os quais, a nível prático nem sempre se mostram operativos.

Por exemplo, em sede de buscas (domiciliárias ou não), é frequente proceder-se à apreensão de sistemas informáticos. Na maioria dos casos, não se demonstra de todo possível obter uma autorização judicial para a recolha das mensagens que possam estar num determinado sistema, dado que nem sempre estas são autorizadas pelo juiz[287]. Havendo autorização judicial para a busca deixaria de levantar o problema da autorização prévia, mas a autorização tem uma finalidade contida na apreensão de elementos que possam servir de prova. O acesso já se encontra num plano diferente, pelo que, na prática, teria valor igual às buscas por iniciativa do Ministério Público ou dos órgãos de polícia criminal. Assim, para CARLOS ADÉRITO TEIXEIRA[288], deverá haver sempre intervenção judicial, mesmo que em momento posterior às buscas, mas sempre anterior ao acesso ao conteúdo por parte do Ministério Público ou dos órgãos de polícia criminal. Portanto, se o acesso for consentido, é possível cumprir com algumas adaptações o preceituado no artigo 188.º[289].

Por fim, relativamente ao catálogo de crimes, alguns mostram não ser compatíveis com a "interceção" do correio eletrónico, em particular os crimes de injúria, ameaça, coação, devassa da vida privada e perturbação da paz e do sossego, na medida em que nos termos do n.º 1 do artigo 187.º implicam que sejam cometidos através do telefone.

Quanto a esta extensão, importa salientar que existe doutrina[290] que considera que a "interceção" do correio eletrónico, na sua fase de transmissão, em todas as investigações em que esteja em causa um crime informático ou um crime do artigo 187.º do CPP, mas que se exija a recolha de prova em suporte eletrónico, faz-se por aplicação das regras devidas à entrada em vigor da LC.

---

[287] Cf. CARLOS ADÉRITO TEIXEIRA, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., pp. 281-282.
[288] Cf. *Ibidem*, p. 283.
[289] Não estão submetidas a este regime as mensagens já impressas em virtude de não se encontrarem, pelo menos em exclusivo, guardadas em suporte digital, mas sim em suporte de papel. Ou seja, cessou o sigilo da comunicação e é por demais evidente (porque estão impressas) que o destinatário deve ter tomado conhecimento da existência da mensagem. Cf. CARLOS ADÉRITO TEIXEIRA, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., pp. 283-284, e ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., pp. 837-838.
[290] Veja-se, por exemplo, RITA CASTANHEIRA NEVES, *As Ingerências nas Comunicações*…, op. cit., pp. 274 e 285.

5.1.6.2 *Short Message Service* (*SMS*)

De acordo com CARLOS ADÉRITO TEIXEIRA[291], o legislador também optou por adaptar o regime das escutas às *sms*[292]. No entanto, considera que, no caso das mensagens escritas, não estamos perante uma interceção, mas sim uma gravação automática do próprio telemóvel, existindo, portanto, várias soluções jurídicas possíveis.

Por um lado, a solução de equiparar o telemóvel a um gravador, e sendo a gravação automática partir-se do pressuposto de que o remetente aceita a gravação da mensagem[293], podendo, assim, a mesma ser utilizada em caso de apreensão do telemóvel ou entrega por parte da vítima.

Por outro lado, podemos equiparar as *sms* a documentos (podendo ser editados ou usados livremente sem pôr em causa o segredo das comunicações) e, por consequência, é indiferente a entrega dos mesmos em suporte papel ou originário (telemóvel), como meio de prova.

Por fim, se tratarmos esta matéria à luz do segredo das correspondências, o regime aplicável será o da apreensão em sede de buscas. Por assim ser, quem deve aceder às *sms* é o juiz de instrução criminal, como referimos para o correio eletrónico, devendo o mesmo fazer uma ponderação semelhante à que faria se estivesse perante uma escuta telefónica. Devem seguir-se, com as devidas adaptações, os procedimentos previstos no artigo 188.º do CPP.

A jurisprudência tem outras interpretações acerca do n.º 1 do artigo 189.º do CPP, as quais se podem estruturar em dois blocos.

Por um lado, tem-se vindo a equiparar as *sms* às vulgares cartas de correio, submetendo-as, se fechadas, ao regime processual penal destas e, se abertas e lidas pelo destinatário, ao regime dos simples documentos[294]. Não se afigura admissível procurar

---

[291] Cf., deste autor, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., pp. 285-288.

[292] Ver, igualmente, PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), p. 527. Importa referir que, segundo o nosso entendimento, quando falamos de *sms* também se incluem as *mms*.

[293] Não belisca o artigo 199.º do CP *ex vi* artigo 167.º do CPP.

[294] Ver o Acórdão do Tribunal da Relação do Porto, de 20-01-2016 (Artur Oliveira), processo n.º 1145/08.4PBMTS.P1, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/54a82f139588437f80257f5a0033e764?OpenDocument, e o Acórdão do Tribunal da Relação de Lisboa, de 24-09-2013 (Vieira Lamim), processo n.º 145/10.9GEALM.L2-5, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c60dfe830c97cf8980257c0000368afa?OpenDocument [consultados a 17-12-2017]. Em sentido contrário, CARLOS ADÉRITO TEIXEIRA,

proteção junto do mecanismo de salvaguarda estabelecido para as escutas telefónicas, porquanto a norma que habilita essa extensão expressamente previa (e prevê) que as conversações ou comunicações fossem transmitidas por meio técnico diferente do telefone, e o telemóvel é ainda um telefone.

Também considera que não podemos estar perante os regimes da pesquisa e apreensão de dados informáticos, quando estes são apresentados por quem os detém ao órgão de polícia criminal e entregues voluntariamente para junção aos autos. Entende-se que não é necessária a autorização do juiz de instrução criminal nesses casos, pois a autoridade policial limita-se a tomar o registo e fazer constar dos autos o teor das mensagens. Por outras palavras, é o destinatário da correspondência que sobre a mesma tem toda a disponibilidade e não o seu remetente. Como destinatário, tem legitimidade para divulgar o seu conteúdo, nomeadamente permitir que as autoridades policiais tenham conhecimento dele [295].

Por outro lado, há jurisprudência que entende que, com a entrada em vigor da LC, este tema passou a ter uma abordagem diferente[296], designadamente se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático. Isto porque, como referiu o Acórdão do Tribunal da Relação de Guimarães, de 29-03-2011 (Maria José Nogueira)[297], não há qualquer razão para que não se possa aplicar às *sms*, de forma direta e imediata, o regime das buscas e apreensões tal como regulado nos artigos 15.º e 16.º da LC. Desde logo, por estar em causa a apreensão de dados informáticos (*sms*) num sistema informático (telemóvel).

«Escutas Telefónicas: A Mudança de Paradigma…», op. cit., p. 287, considera que o n.º 1 do artigo 189.º deverá ser interpretado como "*qualquer meio técnico [mesmo que] diferente do telefone*".

[295] A este propósito, consultar: Acórdão do Tribunal da Relação do Porto, de 20-01-2016 (Artur Oliveira), processo n.º 1145/08.4PBMTS.P1; Acórdão do Tribunal da Relação de Lisboa, de 24-09-2013 (Vieira Lamim), processo n.º 145/10.9GEALM.L2-5; Acórdão do Tribunal da Relação do Porto, de 24-04-2013 (Fátima Furtado), processo n.º 585/11.6PAOVR.P1, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/872f3063233d8de480257b78003e60f3?OpenDocument&Highlight=0,mensagens,sms,artigo,189.%C2%BA, e Acórdão Tribunal da Relação do Porto, de 22-05-2013 (Melo Lima), processo n.º 74/07.3PASTS.P1, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/abf6a7fedb6f7ba580257b88004ed413?OpenDocument&Highlight=0,mensagens,sms,artigo,189.%C2%BA [consultados a 18-12-2017].

[296] Cf. Acórdão do Tribunal da Relação do Porto, de 12-09-2012 (Alves Duarte), processo n.º 787/11.5PWPRT.P1, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/877e0322acde18d080257a8300393cc6?OpenDocument&Highlight=0,mensagens,sms,artigo,189.%C2%BA, e Acórdão do Tribunal da Relação de Guimarães, de 29-03-2011 (Maria José Nogueira), processo n.º 735/10.0GAPTL-A.G1, disponível em http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/6aa96edf91e899b2802578a00054631f?OpenDocument&Highlight=0,mensagens,sms,artigo,189.%C2%BA [consultados a 18-12-2017].

[297] Cf. Processo n.º 735/10.0GAPTL-A.G1.

Nesse caso, deve a autoridade judiciária competente autorizar ou ordenar por despacho que se proceda a uma pesquisa nesse sistema, devendo, sempre que possível, presidir à diligência. Por assim ser, conclui-se, pois, no sentido de carecer de autorização judicial a apreensão de *sms* encontradas no decurso de pesquisa informática ou de outro acesso legítimo a um telemóvel, neste armazenadas.

Não obstante, pode haver ocasiões em que é dispensado o prévio consentimento da autoridade judiciária, estando estas limitadas às situações em que a mesma seja voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique documentado por qualquer forma. Estende-se, ainda, aos casos de terrorismo e de criminalidade violenta ou altamente organizada, quando haja indícios fundados da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.

5.1.6.3 Comunicações entre presentes

O legislador remete o regime das escutas para a comunicação entre presentes, sendo esta remissão clara e inequívoca[298]. Todavia, como refere PAULO PINTO DE ALBUQUERQUE[299], não há uma distinção entre as conversações privadas ditas entre presentes no domicílio ou fora dele, referindo-se a ambas.

Segundo JOÃO GOUVEIA DE CAIRES[300], as comunicações entre presentes são "*o 'olho vivo' que tudo vê. O ouvido que tudo ouve*", por outras palavras as escutas ambientais captam e registam todo um contexto e conteúdo de uma conversa. No entanto, a extensão do artigo 189.º não se aplicará à captação de imagem, mas apenas ao som, pois é o que resulta da sua inserção no regime das escutas telefónicas[301].

---

[298] Crítica esta posição do legislador MANUEL DA COSTA ANDRADE "*não pode ser mais benigno o juízo que nos merece a extensão do regime das intromissões nas telecomunicações à "intercepção das comunicações entre presentes", que nada têm a ver com as telecomunicações. E cuja intercepção, gravação e posterior audição e utilização representam um potencial de devassa e danosidade social claramente superior. A reclamar, por isso, um regime mais consistente e, na perspetiva da introdução, mais exigente e selectivo*.". Cf. *"Bruscamente no Verão Passado" …*, op. cit., p. 186 e também Acórdão do Tribunal da Relação de Guimarães, de 29-03-2011 (Maria José Nogueira), processo n.º 735/10.0GAPTL-A.G1.

[299] Considerando que a interceção das comunicações entre presentes no domicílio é inconstitucional sempre que mantida com pessoas de especial confiança do suspeito ou incluir expressões pertencentes ao núcleo de vida privada do suspeito. Por seu turno, este regime não é aplicável ao monólogo, uma vez que o mesmo não é considerado uma comunicação ou conversação. Cf. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), p. 526.

[300] Cf., deste autor, «O registo de som e imagem…», op. cit., p. 275.

[301] Neste sentido, JOÃO GOUVEIA DE CAIRES. Cf. *Ibidem*, p. 280.

Por sua vez, a Lei n.º 5/2002, de 11 de janeiro, designadamente no artigo 6.º, sob a epígrafe "registo de voz e imagem", de certa forma também regula esta matéria, existindo doutrina[302] que considera que podemos estar perante uma repetição.

Nesse sentido, indicaremos os critérios diferenciadores dos dois regimes: (1) a Lei n.º 5/2002 tem uma autorização reforçada que o regime das escutas telefónicas não tem, designadamente quanto à intrusão da própria intimidade; (2) a Lei n.º 5/2002 não tem limites quanto aos meios utilizados, enquanto o regime das escutas prevê uma tipicidade da sua extensão no artigo 189.º do CPP; (3) a Lei n.º 5/2002 aplica-se sobretudo à imagem, enquanto o regime de escutas se dirige essencialmente à palavra; (4) o catálogo de crimes em ambos os regimes é diferente; e (5) há uma maior exigência de aplicação no regime das escutas do que o previsto na Lei n.º 5/2002, nomeadamente, ser indispensável ou de outra forma ser impossível ou muito difícil, bastando apenas uma necessidade para a investigação. Não obstante, podemos concluir que a recolha de voz e imagem se processa em relação ao catálogo de crimes do n.º 1 do artigo 187.º do CPP, desde que autorizada e controlada pelo juiz, nos termos do artigo 188.º do CPP[303].

5.1.6.4 Registo de comunicações

Segundo o Acórdão do Tribunal da Relação de Évora, de 07-04-2015 (Fernando Pina), processo n.º 13/15.8PAOLH-A[304], os dados como mensagens enviadas ou recebidas, a lista telefónica de contactos, as chamadas recebidas e/ou não atendidas, as chamadas efetuadas, ou outros dados que sejam guardados na memória do telemóvel ou em algum cartão, não necessitam que a sua revelação seja precedida de autorização do juiz de instrução. Com efeito, não se trata aqui de qualquer dado ou comunicação em transmissão, mas apenas um certo dado que se encontra guardado num certo suporte, como o telemóvel ou o cartão de memória.

---

[302] Designadamente, CARLOS ADÉRITO TEXEIRA, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., pp. 288 e ss, e aderindo aos seus fundamentos ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., pp. 838-839, em sentido contrário JOÃO GOUVEIA DE CAIRES considera que é um regime complementar ao do CPP. Cf. «O registo de som e imagem…», op. cit., p. 291.

[303] Neste sentido, está o Acórdão do Tribunal da Relação de Évora, de 08-04-2014 (João Amaro), processo n.º 695/13.5PALGS-A.E1.

[304] Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/ad8068a8c8f9b3c080257e2e00356d33?OpenDocument [consultado a 17-12-2017].

5.1.6.5 Faturação detalhada

A faturação detalhada inclui informações relativas às chamadas efetuadas num determinado período, os números de telefone chamados e a data, a hora e a duração dos telefonemas. A faturação é considerada como dados de tráfego relativos às comunicações efetuadas.

Ora, quanto aos dados, apenas faz sentido exigir-se que seja autorizada a sua obtenção e junção aos autos, uma vez que eles já existem, ao contrário do que acontece nas escutas telefónicas onde estão em causa informações futuras[305].

5.1.6.6 Localização celular

Por fim, o legislador também previu expressamente a localização celular (n.º 2, do artigo 189.º do CPP), estando a mesma sujeita às regras do catálogo de crimes e de sujeitos, bem como à autorização judicial. Todavia, e contrariamente às escutas telefónicas, ela pode ser ordenada em qualquer fase do processo, não se limitando, portanto, ao inquérito[306].

Segundo o Acórdão do Tribunal da Relação do Porto, de 27-02-2013, (Francisco Marcolino), processo n.º 494/09.0GAVLG.P1[307], entende-se por "dados de localização", nos termos da alínea e) do n.º 1 do artigo 2.º da Lei 41/2004, de 18 de agosto, "*quaisquer dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um assinante ou de qualquer utilizador de um serviço de comunicações eletrónicas acessível ao público*". Assim, a localização geográfica ou celular assenta na deteção de aparelhos que se ligam a células disseminadas pelo território e que garantem a cobertura de rede (sem interferir ou intercetar o conteúdo da comunicação) e, em consequência, permitem situar geograficamente o local do aparelho ou a mudança de conexão para outras células, seguindo a trajetória pelas zonas onde o aparelho se encontra a operar. Ou seja, como explica o Acórdão do Tribunal da Relação do Porto, de 11-02-2015 (Neto de Moura), processo n.º 2063/14.2JAPRT-A.P1, a "*localização celular revela a localização de um*

---

[305] Veja-se ANTÓNIO DA SILVA HENRIQUES GASPAR *et al.*, *Código de Processo Penal Comentado*, op. cit., pp. 843-845.

[306] Cf. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), p. 529, e CARLOS ADÉRITO TEXEIRA, «Escutas Telefónicas: A Mudança de Paradigma…», op. cit., p. 291.

[307] Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/42af22f8c0dbc13e80257b2f005e8c70?OpenDocument&Highlight=0,mensagens,sms,artigo,189.%C2%BA [consultado a 18-12-2017].

detentor de telemóvel ou outro equipamento móvel, dando a conhecer o percurso que está a fazer ou fez e a sua mobilidade." [308].

Mais refere o citado aresto de 27-02-2013, e acompanhando o raciocínio de MANUEL DA COSTA ANDRADE, que só os dados autênticos de comunicação, isto é, aqueles que se reportam a comunicações efetivamente realizadas ou tentadas/falhadas entre pessoas, detêm aquele estatuto e regime (de dados de tráfego). Caem, assim, fora do regime e da área de tutela da inviolabilidade das telecomunicações os procedimentos de identificação do número de um aparelho de telemóvel ou do respetivo cartão (IMEI e IMSI). O mesmo é válido para os consequentes dados obtidos, concretamente os dados de localização logrados através destes procedimentos. Isto porque, na verdade, tais procedimentos não pressupõem qualquer ato de comunicação, bastando que o telemóvel esteja em posição *stand-by*, ou seja ligado e apto para receber chamadas.

Por fim, também se levanta a questão do uso de recetores de *GPS*. Como menciona PAULO PINTO DE ALBUQUERQUE[309], a colocação de um recetor de *GPS* no veículo do suspeito ou do arguido não está prevista na extensão ao regime das escutas telefónicas, desde logo porque não há uma comunicação. Por isso, este meio de obtenção de prova não é admissível como meio atípico, visto que deve estar expressamente previsto e considerado o seu elevado grau de intrusão na privacidade do sujeito em causa.

No mesmo sentido, o Acórdão do Tribunal da Relação de Lisboa, de 13-04-2016 (Carlos Almeida), processo n.º 2903/11.8TACSC.L1-3[310], explica que este aparelho, vulgarmente conhecido como "*GPS tracker*", contém, em geral, um módulo de comunicações, além de um recetor de *GPS*. Este, através da utilização de uma tecnologia diferente (eventualmente *GPRS*), permite a transmissão dos dados obtidos pelo recetor para a entidade que instala e controla o mesmo, sendo os dados facultados, em tempo real, à pessoa que contratou este serviço, através da utilização da ligação à *internet*. Ora, "*estes aparelhos e as tecnologias que os mesmos utilizam permitem conhecer, pelo menos, a localização instantânea e precisa do veículo em que se*

---

[308] Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/f2cd9bcbafe3b34080257df7004ca094?OpenDocument [consultado a 18-12-2017].

[309] Cf. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), p. 527.

[310] Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/49e0ed047fc8207280257f9c002e01c9?OpenDocument&Highlight=0,registo,de,comunica%C3%A7%C3%B5es,artigo,189.%C2%BA [consultado a 18-12-2017].

encontram instalados, o percurso pelo mesmo efetuado, os tempos e locais de paragem, o período de funcionamento do motor e a velocidade a que o automóvel circula, podendo propiciar ainda, se tal for pretendido, a obtenção de um leque muito mais alargado de dados, a transmissão de mensagens escritas e o bloqueio da circulação da viatura." Perante o exposto, não é permitida esta técnica, pois consubstancia um meio oculto que só pode ser admitido caso exista lei que o legitime e regule os aspetos do seu regime.

5.1.6.7 Buscas *online*

Por fim, também se poderia cair na 'tentação' de aproveitar a extensão do artigo 189.º do CPP para as buscas *online*. Porém, nem o regime das escutas telefónicas nem o seu artigo 189.º abriu portas a este meio oculto, ou seja, não é possível, através do regime aplicável às escutas telefónicas, infiltrar-se num sistema informático com o intuito de obter informações ou dados[311], em virtude de, tal como acontece para o *GPS*, se impor a reserva de lei e de juízo.

5.2 Ações encobertas

À semelhança da análise efetuada para as escutas telefónicas, neste subtítulo pretendemos desenvolver os requisitos essenciais a fim de que uma ação encoberta seja autorizada. Dito de outro modo, não pretendemos fazer um exame extenso deste meio encoberto, mas antes desenvolver os seus pressupostos fundamentais.

No que a esta matéria diz respeito, é discutido pela doutrina e pela jurisprudência a figura do agente infiltrado e do agente provocador e, em resultado, a sua responsabilidade penal. Contudo, por entendermos que esta discussão ultrapassa o objetivo da presente análise, optámos por não abordar estas questões.

Nos termos do n.º 2 do artigo 1.º do Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal, são consideradas ações encobertas "*aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiro atuando sob o controlo da Polícia Judiciária para prevenção ou repressão dos crimes indicados nesta lei, com ocultação da sua qualidade e identidade*". Por seu turno,

[311] Cf. PAULO PINTO DE ALBUQUERQUE, *Comentário do Código de Processo Penal*…, op. cit. (2.ª edição), p. 527, ANTÓNIO DA SILVA HENRIQUES GASPAR *et al*., *Código de Processo Penal Comentado*, op. cit., p. 835, e PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, op. cit., p. 89.

conforme refere EDUARDO MAIA COSTA[312], a tarefa dos agentes encobertos é introduzirem-se no meio dos arguidos ou suspeitos, sempre sem revelar a sua verdadeira identidade e objetivos, tentando ganhar a confiança daqueles, de modo a eventualmente integrarem a organização criminosa, ou poderem acompanhar as atividades ilícitas. Deste modo, obtêm informações e recolhem indícios e elementos de prova das infrações em investigação, as quais tanto podem estar já consumadas como estar em fase de execução ou preparação[313].

Em suma, estamos perante um meio insidioso, que lesa uma grande quantidade de direitos fundamentais, quer do sujeito quer de outras pessoas. Está em causa a própria integridade moral, prevista no n.º 1 do artigo 25.º da CRP, quer pela intromissão dissimulada na vida privada ou mesmo na intimidade, quer pela manipulação do sujeito visado. Por sua vez, lesa também direitos como ao silêncio e não autoincriminação, e princípios como os da transparência, lealdade de atuação da entidade que investiga e acusa e igualdade de armas entre sujeitos processuais[314]. Como não existem princípios ou valores absolutos, em situações determinadas estes 'cedem' para salvaguardar valores conflituantes, como é o caso da segurança coletiva ou individual, e busca da verdade material.

Nesse caso, é necessário respeitar as regras da estrita excecionalidade e proporcionalidade entre a gravidade da conduta e os meios previstos para a investigação criminal. Significa isto que é exigida uma prévia ponderação do legislador aquando da redação da lei e, posteriormente, uma segunda reflexão da autoridade que autoriza.

Em síntese, tal como prevê o n.º 1 do artigo 3.º do Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal, a ação encoberta terá de ser adequada aos fins de prevenção e repressão criminal identificados em concreto, e proporcional ao fim que se pretende e à gravidade do crime que se investiga.

---

[312] Cf. EDUARDO MAIA COSTA, «Ações encobertas (Alguns problemas, algumas sugestões)», *in* AA.VV., *Estudos em Memória do Conselheiro Artur Maurício*, org. Maria João Antunes, Coimbra, Coimbra Editora, 2014, p. 364.

[313] Na vizinha Espanha, a tarefa dos agentes encobertos é semelhante à nossa. Passa por eles se infiltrarem em organizações criminosas, desempenhando um papel que confunda os seus membros, permitindo-lhes acreditar que se trata de um deles, a fim de obter informações ou provas que possam impedir a execução do crime ou sancionar o crime já consumado. O normativo espanhol prevê também que os agentes possam recorrer a uma qualquer forma de introdução, desde que não lesem os direitos fundamentais dos sujeitos investigados. Cf. Acórdão do Supremo Tribunal, de 15-11-2007, STS 7815/2007, disponível em http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=259097&links=&optimize=20071220&publicinterface=true [consultada a 08-12-2017].

[314] Cf. EDUARDO MAIA COSTA, «Ações encobertas...», op. cit., p. 358.

Ora, para a determinação de uma ação encoberta, têm de estar consagrados os pressupostos materiais da adequação, proporcionalidade e subsidiariedade. Ou seja, não basta estarmos perante um crime do catálogo; é necessário que a ação seja apta a obter o resultado pretendido, seja proporcional à gravidade concreta do crime investigado (tem de existir uma proporcionalidade em sentido estrito entre a "gravidade da ação" e a "gravidade do crime") e, por fim, que seja exatamente necessária (isto é, não ser possível outro meio de obtenção de prova ter a eficácia desejada). Estes pressupostos são cumulativos, uma vez que só a sua verificação garante o carácter excecional das ações encobertas e a sua legitimidade como meio oculto de investigação.

Por todo o exposto, as ações encobertas só podem ser autorizadas quando forem indispensáveis para assegurar os fins de prevenção e repressão, e quando nenhum outro meio for eficaz.

5.2.1 Fase do processo e competência

Para além dos requisitos materiais acima referidos, é necessário estarmos perante as condições de validade previstas nos n.ºs 3 a 6 do artigo 3.º do Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal.

Quanto à fase do processo, e distintamente das escutas telefónicas, as ações encobertas tanto podem ser realizadas com a finalidade de prevenção como de repressão[315]. Por seu turno, a competência para as determinar depende diretamente do momento em que se encontra o processo – pré-inquérito ou inquérito.

No âmbito do inquérito, este meio tem de ser previamente autorizado pelo magistrado do Ministério Público e comunicado ao juiz de instrução criminal, considerando-se validado se não for proferido despacho de recusa em setenta e duas horas (n.º 3 do artigo 3.º do supracitado Regime Jurídico). Se tivermos perante fins de prevenção criminal, a ação terá que ser expressamente autorizada pelo juiz de instrução criminal, mediante proposta do Ministério Público.

No âmbito do pré-inquérito, isto é, se a ação tiver uma finalidade preventiva estrita, a iniciativa é do magistrado do Ministério Público junto do Departamento Central de Investigação e Ação Penal, e tem de ser expressamente autorizada pelo juiz

[315] Como refere PAULO DE SOUSA MENDES, «Investigação, prevenção e informação de segurança», *in* Manuel Monteiro Guedes Valente (coord.), *IV Congresso de Processo Penal – I Congresso Luso-Brasileiro de Criminalidade Económico-Financeira*, Coimbra, Almedina, 2016, p. 70, é a doutrina que terá de contribuir para uma demarcação clara entre a prevenção e a investigação criminal, porque no âmbito das ações encobertas há uma indefinição, o que facilita que as ações de prevenção se transformem em pré-averiguações sem a direção do Ministério Público.

do Tribunal Central de Instrução Criminal (n.º 5 do artigo 3.º). O critério de ponderação será a forte probabilidade de vir a ser instaurado o inquérito, por força do conceito de indícios suficientes previsto no n.º 2 do artigo 283.º do CPP[316].

A proposta para a realização de uma ação encoberta deverá ser devidamente fundamentada, dirigida em envelope fechado ao titular da ação penal, descrevendo-se a realidade criminal emergente que carece deste meio especial e excecional. Se estivermos em fase de inquérito, a proposta deverá dar conta de um conjunto de acontecimentos suscetíveis de configurar um crime do catálogo, o qual pela sua especial complexidade, gravidade e grau organizacional requer o recurso a este meio de obtenção de prova. Independentemente de estarmos em fase de inquérito ou de pré-inquérito, o oferecimento deverá contextualizar os factos em causa, explicando a excecionalidade do meio face à impossibilidade de se obter prova por outro menos lesivo, definir um plano de ação e concretizar a finalidade de obtenção de material probatório ou de obviar à continuação da atividade delituosa[317].

O despacho do Ministério Público conterá uma ponderação dos bens jurídicos em causa e todo o circunstancialismo, e determinará os atos autorizados a praticar pelo agente encoberto. Durante a ação encoberta, o titular da ação penal procederá à reavaliação dos pressupostos, decidindo quanto à autorização de novos atos[318].

Por último, e porquanto concordamos com esta posição, não podemos deixar de referir que existe doutrina[319] referente à competência para determinar a ação, a qual critica a decisão do legislador. Considera essa doutrina que a intervenção do juiz, quando estamos em fase de inquérito, é mitigada pela "invulgar validação tácita". Também não compreende como é que um meio tão lesivo de direitos fundamentais permite tal validação, quando o papel do juiz se afigura indispensável para a garantia da tutela preventiva dos direitos. Indaga, igualmente, o porquê de não se seguir o que está previsto para as escutas telefónicas – autorização prévia do juiz de instrução criminal e não a sua convalidação.

---

[316] Cf. RUI PEREIRA, «O *Agente Encoberto* na Ordem Jurídica Portuguesa», *in* AA.VV., *Estudo em Homenagem ao Conselheiro José Manuel Cardoso da Costa,* volume II, Coimbra, Coimbra Editora, 2005, p. 298.

[317] Cf. DANIEL SILVA, «Ações encobertas no Estado de Direito Democrático», *Investigação Criminal*, número 5, maio de 2013, pp. 54-55.

[318] Cf. *Ibidem*.

[319] Neste sentido, veja-se RUI PEREIRA, «O *Agente Encoberto* na…», op. cit., p. 298, e EDUARDO MAIA COSTA, «Ações encobertas…», op. cit., pp. 363-364.

Nesse sentido, EDUARDO MAIA COSTA[320] refere que a autorização tácita, por não ser acompanhada de fundamentos, viola o princípio da obrigatoriedade de fundamentação dos atos jurisdicionais (n.º 3 do artigo 97.º do CPP e n.º 1 do artigo 205.º da CRP). Acrescenta que só uma atuação pré-definida pode garantir o respeito pelos princípios assinalados da adequação, proporcionalidade e subsidiariedade. Pelo que é imperativo, tal como acontece para a escutas telefónicas, haver fundamentação da autorização, conhecendo, em consequência, o agente encoberto qual o plano em que se pode mover e a duração da ação, entre outros.

Relativamente à fiscalização judicial, deveria existir um relatório, como acontece com as escutas telefónicas, pelo menos quinzenal, onde se controlasse a atuação do agente encoberto e se tomasse conhecimento de todo o circunstancialismo da ação.

Prevê o n.º 6 do artigo 3.º Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal, a entrega de um relato do agente encoberto ao Ministério Público ou ao juiz no prazo de quarenta e oito horas após o termo da ação, não tendo o legislador detalhado o modo da sua elaboração. Sabemos que este relato não tem qualquer valor probatório[321]. Senão vejamos.

A autoridade judiciária ordenará a junção do relato ao processo, somente se for absolutamente indispensável em termos probatórios, conforme o n.º 1 do artigo 4.º do Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal.

Por sua vez, o agente encoberto só poderá intervir como testemunha, se o juiz determinar a sua extrema necessidade para a produção de prova.

Podemos assim concluir que, à partida, a ação encoberta não será dada a conhecer ao arguido, salvo no caso de o relato ser junto aos autos ou quando o agente encoberto tiver intervenção como testemunha. Significa isto que há uma manifesta redução das garantias de defesa do arguido[322].

---

[320] Cf., deste autor, «Ações encobertas…», op. cit., p. 363.

[321] Neste sentido, podemos verificar no Acórdão do Tribunal da Relação de Lisboa que quando o relato não é junto aos autos ele não pode ter qualquer valor probatório. Também se demonstra neste aresto que a regra é a de não dar a conhecer ao arguido a existência de uma ação encoberta. Cf. Acórdão do Tribunal da Relação de Lisboa, de 25-05-2010 (Pedro Martins), processo n.º 281/08.1JELSB.L1-5, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/a330ce544a1b3a3f8025779f00478de4?OpenDocument&Highlight=0,agente,encoberto,a%C3%A7%C3%B5es,encobertas [consultado a 19-12-2017].

[322] Muito crítico desta posição é EDUARDO MAIA COSTA. Cf., deste autor, «Ações encobertas…», op. cit., pp. 366-368. Em Espanha, também se entende que o não depoimento do agente encoberto deverá ser a exceção e não a regra. Com efeito, a sujeição do arguido a tal grau de lesão tem de ser compensada de forma adequada e razoável. O TEDH já se pronunciou também neste sentido. Cf. ÁLVARO REDONDO

5.2.2 Catálogo de crimes

Este meio oculto de investigação criminal só poderá ser aplicado no âmbito de um catálogo taxativo de crimes que se encontra previsto no artigo 2.º do Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal. Quer dizer, só nesses casos é que as ações encobertas podem ser praticadas.

O catálogo é extenso e abrange crimes, designadamente contra as pessoas, o património, a vida em sociedade e contra ao Estado, sendo, por conseguinte, variável a pena aplicável em abstrato. Como referiu FIGUEIREDO DIAS[323], este regime jurídico carateriza-se por ser uma lei mais de intenções do que de resultados, dado que o catálogo de crimes por ela apresentada está associado a crimes de alta gravidade, mas não só, verificando-se algumas indefinições jurídicas.

Posteriormente, com a entrada em vigor da LC, o catálogo de crimes foi alargado por força do n.º 1 do artigo 19.º. Ora, se ele já era extenso em medidas de pena medianas, esta lei veio acentuar ainda mais a desigualdade de danosidade penal. Passou a ser permitido: o recurso às ações encobertas nos casos da falsidade informática; dano relativo a programas ou outros dados informáticos; sabotagem informática; acesso ilegítimo; interceção ilegítima; reprodução ilegítima de programa protegido; crimes cometidos por meio de sistema informático, quando lhes corresponda, em abstrato, pena de prisão de máxima superior a 5 anos, ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos.

Como refere PAULO DÁ MESQUITA, transigiu-se a linha do admissível quando se previu uma medida de carácter muito excecional para um leque muito amplo de crimes, sem aprofundamento normativo dos princípios da proporcionalidade e da necessidade. Admite-se "*quaisquer acções encobertas para um amplo catálogo de crimes, alguns dos quais integrados na pequena criminalidade (por via da al. a) do n.º 1, para os tipos dos arts. 3.º, n.º 1, 5.º, n.os 1 e 2, 6.º, n.os 1 e 3, 7.º, n.os 1 e 2, da lei do*

HERMIDA, «El *agente encubierto* en la Jurisprudencia española y en la doctrina del Tribunal Europeo de Derechos Humanos», *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, número 45, janeiro de 2008, p. 10.

[323] Ver «O Processo Penal Português: Problemas e Prospectivas», op. cit., p. 811.

cibercrime, e por via da al. b) do n.º 1 do art. 19.º para um elenco de crimes com penas máximas até 5 anos «sendo dolosos»), parecendo ainda pretender-se o emprego da medida para crimes negligentes com pena superior a 5 anos (um absurdo inerente à previsão da al. b) do n.º 1 art. 19.º de ressalva dos crimes dolosos puníveis até 5 anos)."[324].

5.2.3 Determinação do agente encoberto

O agente encoberto pode ser um funcionário de investigação criminal ou um terceiro, desde que atuando sobre o controlo desta entidade, conforme n.º 2 do artigo 1.º do Regime Jurídico das Ações Encobertas para Fins de Prevenção e Investigação Criminal.

Os funcionários de investigação, tanto podem ser da Polícia Judiciária, Polícia de Segurança Pública, Guarda Nacional Republicana e Serviço de Estrangeiros e Fronteiras, mas estes últimos apenas quanto ao âmbito de crimes relacionados com a imigração ilegal por associações criminosas[325].

Por seu turno, só o agente policial poderá atuar sob identidade fictícia, porque tal atribuição pressupõe um grau de confiança muito elevado na pessoa que a assume. A identidade é atribuída por despacho do Ministério da Justiça, mediante proposta do Diretor Nacional da Polícia Judiciária. Esta identidade é válida por um período de seis meses, prorrogáveis por igual período.

Por último, os terceiros são os denominados "homens de confiança". Como refere EDUARDO MAIA COSTA[326], o recurso a eles não é pacífico, visto não existir um vínculo de fidelidade ao Estado que, contrariamente, é inerente ao funcionário de investigação. Esta figura não constitui uma garantia absoluta de fidelidade.

5.2.4 Prazo de autorização

O legislador não estipulou um prazo de autorização, como acontece para as escutas telefónicas. Contudo, no n.º 3 do artigo 5.º, confere um prazo de validade para a identidade fictícia (seis meses, prorrogável por igual período).

Assim, a este propósito, existem várias interpretações. Por um lado, e apesar da ação encoberta correr paralelamente ao inquérito, há quem considere que o prazo

---

[324] Cf. PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, op. cit., p. 126.
[325] Cf. EDUARDO MAIA COSTA, «Ações encobertas…», op. cit., p. 362.
[326] Cf. *Ibidem*.

máximo será o da duração do inquérito[327], não podendo a mesma ser renovada depois desse período. Por outro, há quem entenda que o prazo é autónomo e distinto do previsto para o inquérito, podendo o mesmo ser ultrapassado.

Na nossa opinião, o prazo máximo deverá ser o da duração do inquérito, mas mantendo-se a ação encoberta se já iniciada antes do seu termo.

5.2.5 Agente encoberto na *internet*

Embora, à partida, não esteja regulada a figura do agente encoberto *online*[328], podemos também fazer referência a ela[329]. No nosso entendimento, esta deverá basear-se na figura do tradicional agente encoberto, tendo como intuito infiltrar-se na rede para obter informações sobre os autores de determinados crimes. Tudo isto através da criação de um perfil falso que permite estabelecer relações de confiança e integrar-se no mundo do "cibercrime", obtendo as informações necessárias para haver uma incriminação.

Em termos de procedimento, deverá obedecer ao mesmo género de requisitos previstos para as ações encobertas[330], devendo o juiz no despacho de autorização indicar os termos do perfil a ser criado, nomeadamente, nome, idade, descrição e modo de atuação.

Em Espanha, esta figura encontra-se prevista nos n.ºs 6 e 7 do artigo 282 *bis* da *Ley de Enjuiciamiento Criminal*[331] e é utilizada para um catálogo taxativo de crimes. A competência para autorizar este meio cabe ao juiz de instrução. Por sua vez, é ao Ministério do Interior que cabe autorizar a criação do perfil falso, sendo o mesmo válido por um período de seis meses, renovável por igual período.

Por último, deve dar-se grande importância ao *nickname* escolhido, devendo estar associado aos crimes em investigação.

Contudo, como refere FEDERICO BUENO DE MATA[332], no caso da pornografia infantil, este método surge com alguns problemas, porque é prática habitual

---

[327] Neste sentido, ver EDUARDO MAIA COSTA, «Ações encobertas…», op. cit., p. 363.
[328] Discutiremos esta questão no capítulo seguinte.
[329] Com certeza, ela é usada fora das malhas da lei.
[330] Evidentemente, corrigidas as lacunas já assinaladas.
[331] Pode verificar-se a sua utilização no Acórdão do Supremo Tribunal, de 05-10-2017, STS 3565/2017, disponível em http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=8171559&links=agente%20encubierto%20inform%C3%A1tico&optimize=20171020&publicinterface=true [consultado a 19-12-2017].
[332] Ver «Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿deberían ampliarse las actuales funciones del agente encubierto en internet?», *El processo penal en la sociedad de*

entre os utilizadores desse estilo de *websites* enviar conteúdos pornográficos, a fim de ganharem a confiança e provarem a lealdade. Ora, nesse caso, estaríamos, por um lado, a cometer um crime ao enviar fotografias/vídeos de menores de cariz sexual e, por outro, corríamos o risco de ao utilizarem-se vídeos de maiores de idade com aparência de menores, os mesmos serem vazados na *internet*.

Em conclusão, esta análise permite aferir que num regime jurídico é importante, entre outros: (1) verificar que o meio é utilizado como último recurso, e é adequado e proporcional ao caso concreto; (2) apontar o catálogo de crimes; (3) definir a competência judicial para autorização da diligência; (4) delimitar o catálogo de sujeitos; (5) restringir a duração; (6) efetuar o acompanhamento e controlo judicial; e (7) dar a conhecer ao arguido o recurso à medida.

---

la información: Las nuevas tecnologías para investigar probar el delito, coord. Julio Pérez Gil, Madrid, *La Ley*, 2012, p. 7.

6. O *malware* e a lei do cibercrime

Não queremos concluir esta dissertação sem averiguar se no nosso atual regime jurídico o uso de *malware* encontra ou não previsão, o que faremos de seguida.

Antes de mais, importa salientar que, tal como afirma MANUEL DA COSTA ANDRADE[333], o recurso a *software* malicioso (ou a "buscas *online*", nas palavras deste autor), como meio de obtenção de prova, não está previsto na lei processual penal vigente, pelo que a excluímos desta discussão. A questão que ora se levanta é se este meio oculto foi admitido na LC.

Como referimos no primeiro capítulo, deu entrada no Parlamento a Proposta de Lei n.º 289/X/4.ª, a 20 de maio de 2009, cuja exposição de motivos mencionava a pretensão da Convenção sobre Cibercrime do Conselho da Europa para harmonizar as várias legislações nacionais sobre a matéria, propiciar e facilitar a cooperação internacional e simplificar as investigações de natureza criminal. Para o efeito, seriam 'importadas' novas formas de investigação e novas vias de cooperação, estas últimas quando necessárias. Em consequência, a lei vigente seria alterada.

A proposta supracitada baixou, no dia seguinte, à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, e foi votada a 1 de julho de 2009, na Reunião da Comissão n.º 137. O relatório desta Comissão foi enviado ao Presidente da Assembleia da República, e a sua discussão na generalidade ocorreu a 9 de julho seguinte.

Neste âmbito, o Senhor Deputado Fernando Negrão (PSD) questionou o Senhor Secretário de Estado acerca do motivo por que o diploma não contempla a possibilidade de as entidades de investigação introduzirem no sistema informático sob investigação "cavalo de Tróia informático", a fim de obter informação contínua e em tempo real, e facilitar as investigações. Não tendo obtido resposta, o Senhor Deputado reiterou a questão, ao que lhe foi respondido: "*Sr. Deputado, o Sr. Secretário de Estado também já não dispõe de tempo para responder. Talvez possa fazê-lo noutra altura, porventura na sequência dos trabalhos em sede de especialidade, se for caso disso*."[334].

Posteriormente, a Comissão deliberou incumbir a um grupo de trabalho, constituído pelos Senhores Deputados Ricardo Rodrigues (PS), Fernando Negrão

---

[333] Ver *"Bruscamente no Verão Passado"* …, op. cit., p. 150.
[334] Cf. Diário da Assembleia da República, I Série, n.º 102/X/4, de 09-07-2009, pp. 40-45, disponível em http://debates.parlamento.pt/catalogo/r3/dar/01/10/04/102/2009-07-10/40?pgs=40-45&org=PLC [consultado a 25-10-2016].

(PSD), António Filipe (PCP), Nuno Magalhães (CDS - PP), Helena Pinto (BE) e Heloísa Apolónia (PEV), a preparação da discussão e votação na especialidade daquela iniciativa legislativa. O referido grupo de trabalho discutiu as soluções normativas da proposta de lei e as propostas de alteração, e votou-as indiciariamente. O projeto de texto final foi remetido à consideração da Comissão, para apreciação e ratificação das votações indiciárias alcançadas e para votação das normas.

A 29 de julho de 2009, o diploma baixou à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias para a redação final. No dia seguinte, foi votado o texto na Reunião da Comissão n.º 143. Por fim, o Decreto da Assembleia n.º 373/X viria a aprovar a LC.

Em suma, durante a discussão na especialidade, a questão colocada pelo Senhor Deputado Fernando Negrão não foi mais suscitada, pelo que nenhuma resposta foi dada acerca da possibilidade de as entidades de investigação criminal recorrerem ao uso de *malware* para obtenção de prova. Ora, a derradeira questão será: está o *malware* previsto na LC?

6.1 A existência de norma habilitante

Segundo DAVID SILVA RAMALHO, o recurso ao *malware* está consagrado no artigo 19.º, sob a epígrafe ações encobertas, designadamente no n.º 2 da LC[335], o qual prevê que "*sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a interceção de comunicações*".

Para este autor, os "meios e dispositivos informáticos", referidos no n.º 2, não se subsumem a qualquer um dos meios de obtenção de prova previstos na nossa legislação. Pelo contrário, a norma surge para colmatar a insuficiência dos demais meios processuais existentes e, em consequência, permite a utilização destes novos meios e dispositivos informáticos[336]. Não se trata de dispositivos eletromagnéticos, acústicos, mecânicos ou outros utilizados no conceito de interceção da alínea e) do artigo 2.º da LC, mas sim de um outro meio que visa recolher prova de um modo

---

[335] "*Entendemos que o uso de malware como meio de obtenção de prova está já consagrado no ordenamento jurídico nacional, em particular no artigo 19.º, n.º 2, da Lei do Cibercrime*". Cf. DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., p. 304. Refira-se que o n.º 2 não estava previsto na Convenção sobre Cibercrime do Conselho da Europa, tendo sido uma iniciativa portuguesa.

[336] Cf. *Ibidem*, p. 310.

inadmissível até à sua entrada em vigor[337]. Estamos, segundo este autor, perante "*meios e dispositivos que operam de modo materialmente semelhante à figura do agente encoberto […] e que devem ser utilizados quando a própria ação encoberta e os demais métodos ocultos forem incapazes de dar respostas às exigências da investigação. Trata-se […] da consagração do hacking e da utilização […] de malware como método oculto de investigação criminal em ambiente digital*."[338].

O autor fundamenta ainda a sua posição no uso de uma terminologia semelhante por parte de diplomas de outros ordenamentos jurídicos, a saber: "meios técnicos", no § 5.2 (11) da Lei de Proteção da Constituição da Renânia do Norte-Vestefália; "dispositivos técnicos", no artigo 706-102-1 do CPP francês; e "dispositivos de vigilância de dados", no artigo 6.º do *Surveillance Devices Act* australiano[339].

Em síntese, o autor defende que o regime jurídico do *malware* decorre da interpretação do normativo das ações encobertas, conjugado com o da interceção das comunicações. Deste modo, o seu uso só é admitido no âmbito das ações encobertas, ou seja, tanto para fins de prevenção como repressão criminais, desde que proporcionados a essa finalidade, bem como à gravidade do crime em investigação. Também só deverá ser utilizado caso haja fundada suspeita da prática de um crime previsto no catálogo, isto é, o previsto para a LC e o do artigo 19.º da mesma lei, e caso seja necessário ou se houver razões para crer que esta diligência é indispensável à descoberta da verdade material ou, em alternativa, que a prova seria impossível ou muito difícil de obter. Por fim, a verificação dos pressupostos deverá constar de despacho fundamentado do juiz de instrução, mediante requerimento do Ministério Público.

Importa recordar que, nem sempre, DAVID SILVA RAMALHO defendeu esta posição de forma tão manifesta. Em 2013, quando se pronunciou pela primeira vez sobre esta questão, defendeu que, ao concluir-se que o n.º 2 do artigo 19.º da LC previa o uso de *malware*, não se podia concordar com os moldes em que o mesmo tinha sido consagrado. Este meio, devido ao seu elevado nível de danosidade social e à gravíssima ofensa dos direitos fundamentais em causa, teria de ter uma consagração legal densa, bem como uma clarificação das suas funcionalidades. Por sua vez, não bastava a existência de uma norma para conferir suporte legal à utilização de *malware*, porquanto,

[337] Cf. *Ibidem*, pp. 310-311.
[338] Cf. *Ibidem*, p. 312.
[339] Cf. *Ibidem*.

em medidas desta natureza, tanto era importante a reserva de lei como a reserva de precisão legal.

Neste caso, considerou o autor que o dever de precisão legal não seria compatível com a mera criação de um meio de investigação cujo funcionamento e finalidade não eram (são) referidos na própria norma que os prevê. Acrescentou que a "*utilização de malware não se compadece com uma mera referência à sua necessidade, seguida de uma remissão genérica 'naquilo que for aplicável' para um regime legal que, por sua vez, remete 'em tudo o que não for contrariado' para outro regime.*" [340]. Contrariamente, seria necessária a qualidade de lei, como já referiu o TEDH em outras ocasiões. Concluiu, assim, pela inconstitucionalidade da norma, por violação do disposto no n.º 2 do artigo 18.º, n.º 2 do artigo 26.º, e artigo 1.º, todos da CRP[341].

Por seu turno, JOÃO CONDE CORREIA também defendeu que o *malware* como meio de obtenção de prova já é hoje permitido, concretamente, pelo n.º 2 do artigo 19.º da LC. Argumenta a sua posição no elemento gramatical, isto é, que as buscas *online* resultam da possibilidade de recorrer "*a meios e dispositivos informáticos*". Refere, contudo, que a letra da lei baliza a possibilidade de recurso a este meio, nomeadamente ao âmbito das ações encobertas. Mas acaba por criticar o facto de não ser possível utilizá-lo nas expressões mais graves de criminalidade e questiona o catálogo de crimes em que é admitido este método[342].

FRANCISCO MARCOLINO DE JESUS também defende que o uso de *malware* está previsto na LC, quando afirma que a "*Lei 109/2009, de 15/09, ao que se crê, permite a busca online.*"[343]. Porém, não esclarece em que normativo considera encontrar-se inserido este método. Acrescenta que no caso de não se entender que a norma tenha suficiente densidade, o meio não pode ser utilizado, pois violaria o princípio da legalidade.

Por último, referimos PAULO PINTO DE ALBUQUERQUE, como igual defensor da previsão do uso de *malware* na LC. Considera que "*a busca online foi agora consagrada pelo novo artigo 15.º da Lei n.º 109/2009, de 15.9*", o qual prevê a

---

[340] Cf. DAVID SILVA RAMALHO, «O uso de *malware*…», op. cit., p. 234.
[341] ID, *ibidem*, p. 234.
[342] Apesar de o autor utilizar o conceito de buscas *online*, podemos concluir, face à seguinte descrição apresentada, que se refere ao conceito de *malware*: "*mediante várias técnicas informáticas à distância, via internet, aceder aos dados contidos num computador, observá-los, monitoriza-los, copiá-los sem o conhecimento e consentimento do visado.*". Cf. JOÃO CONDE CORREIA, «Prova digital: as leis que temos e a lei que devíamos ter», op. cit., pp. 42 e ss.
[343] Cf., deste autor, *Os Meios de Obtenção da Prova em Processo Penal*, 2.ª edição, Coimbra, Almedina, 2015, p. 246.

possibilidade de uma pesquisa informática, por despacho da autoridade judiciária ou mesmo decisão do órgão de polícia criminal. Mais adianta que, a nova lei não coloca quaisquer restrições no que diz respeito aos conteúdos dos dados que podem ser pesquisados, como acontece na apreensão informática, nem exige que a pesquisa, quer seja ordenada pelo Ministério Público quer pelos órgãos de polícia criminal, seja validada pelo juiz. Conclui, todavia, que esta intrusão na privacidade da pessoa lesada é desproporcional, face aos n.ºs 1 e 2 do artigo 26.º e n.º 4 do artigo 32.º da CRP, os quais reservam ao juiz os atos instrutórios que representem uma intrusão na privacidade[344]. Ora, o artigo 15.º da LC será inconstitucional, na medida em que permite ao Ministério Público ou aos órgãos de polícia criminal ordenar o uso de *malware* sem o controlo prévio ou posterior de um juiz. Exceto, nos casos em que os dados íntimos ou privados sejam submetidos ao juiz para os efeitos do n.º 3 do artigo 16.º, validando este, consequentemente, a técnica.

6.2 A inexistência de norma habilitante

Já noutra perspetiva, RITA CASTANHEIRA NEVES[345] considera que na LC não está consagrada a possibilidade de recurso ao *malware*. De acordo com as suas palavras, nem no artigo 15.º nem no artigo 16.º da LC se verifica a possibilidade de se efetuarem buscas *online*, no sentido de poderem ser recolhidos dados informáticos sem conhecimento do visado. Por um lado, o n.º 1 do artigo 15.º faz referência à presença da autoridade judiciária na diligência, o que é incompatível com a natureza oculta do meio. Por outro, as formas de apreensão do n.º 7 do artigo 16.º deixam de fora a possibilidade de as instâncias formais de controlo poderem levar a cabo buscas sem o visado se aperceber disso. Por fim, ao serem admitidas as buscas *online* nestes termos, estaríamos perante uma violação do princípio da legalidade.

Nesse mesmo sentido, PAULO DÁ MESQUITA[346] considera que não se pode confundir a utilização de *malware* com os regimes previstos nos artigos 15.º e 16.º da LC, os quais se aplicam às pesquisas e apreensões informáticas. Apesar da terminologia da LC, continua-se a aplicar o n.º 1 do artigo 174.º do CPP, isto é, quando existirem indícios de que os dados informáticos relacionados com um crime ou que possam servir

---

[344] Cf., deste autor, *Comentário do Código de Processo Penal*…, op. cit. (4.ª edição), p. 502.
[345] Veja-se, *As Ingerências nas Comunicações*…, op. cit., pp. 272-273 e 284.
[346] Cf., deste autor, PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, op. cit., p. 115. Em sentido diferente, como refere DAVID SILVA RAMALHO, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., pp. 305 e 308, há autores que admitem o *malware* com base na aplicação do regime previsto nestes dois artigos.

de prova estejam num determinado sistema informático, é ordenada uma busca informática. Já no que diz respeito às apreensões, os pressupostos continuam a ser os dos n.ºs 1 e 3 do artigo 178.º do CPP. Ou seja, são apreendidos os sistemas informáticos e os dados informáticos que tiverem servido ou fossem servir à prática de um crime. Ante o exposto, não existe espaço para a instalação e utilização de *software* malicioso.

Por seu turno, acompanhando o raciocínio de MANUEL DA COSTA ANDRADE[347], também não se pode permitir o recurso ao *malware* (ditas "buscas *online*"), por força do artigo 18.º da LC. Isto, porque a busca *online* não configura, pelo menos exclusivamente, uma invasão ou devassa de um ato de telecomunicação, não podendo, em consequência, estar abrangida por normas relativas à interceção das telecomunicações.

Por fim, mas não menos importante, AUGUSTO SILVA DIAS afasta, de modo liminar, a possibilidade de utilização de *malware*, quer por força do artigo 15.º quer dos artigos 18.º e 19.º da LC[348].

Relativamente ao artigo 15.º da LC, estranha que este meio se encontre nesta lei, dado que o regime é muito semelhante ao das buscas não domiciliárias do artigo 174.º do CPP. Acresce que este regime exclui, desde logo, a obtenção de dados em tempo real, bem como a infiltração através de dispositivos informáticos. Por último, este artigo faz depender a pesquisa de dados do despacho da autoridade judiciária, o que não é compatível com o grau de danosidade que o *malware* reveste. Como adianta SILVA DIAS, o emprego de *malware* exige a reserva do juiz.

No que diz respeito ao artigo 18.º da LC, este reporta-se à interceção de comunicações, figura que não reflete a utilização de *malware*. Através deste método oculto é possível aceder a dados armazenados no próprio sistema informático e à atividade do utilizador em tempo real, independentemente da mesma ser enquadrável no conceito de comunicação. Ora, o uso de *malware*, podendo ser um ato de comunicação, não incide forçosamente sobre tal atividade. Portanto, fica também excluída a sua previsão neste regime.

AUGUSTO SILVA DIAS também discorda que o emprego de *malware* encontre a sua regulamentação no artigo 19.º, nomeadamente no seu n.º 2. Para este

---

[347] Cf. *"Bruscamente no Verão Passado"* …, op. cit, pp. 160 e 168.

[348] De acordo com a sua opinião verbal, expressa na comunicação "O uso de *malware* como meio de obtenção de prova", proferida na Conferência *A prova Digital em Processo Penal* ocorrida na Faculdade de Direito da Universidade de Lisboa, em 24 de maio de 2017.

autor, o que está aqui em causa é o recurso ao agente encoberto *online*[349]. Ou seja, o agente encoberto pode operar em ambiente digital, desde que se comprove a necessidade do recurso a meios e dispositivos informáticos.

Neste caso, o problema será então 'desmontar' o conceito de meios e dispositivos informáticos. Para SILVA DIAS não devem ser quaisquer uns, pois a ação encoberta não pode servir de "cheque em branco" para a utilização de meios e dispositivos ocultos, sobre os quais não recaiu, especificamente, uma valoração do legislador. Ora, como o n.º 2 manda aplicar à prova recolhida através da utilização de meios e dispositivos informáticos o regime de interceção das comunicações, com as devidas adaptações, considera AUGUSTO SILVA DIAS que o legislador, ao prescrever tal regime à prova recolhida pelo agente encoberto em meio digital, parece referir-se a meios e dispositivos adequados para intercetar comunicações, o que afasta o uso de *malware*. Ou seja, os meios e dispositivos contemplados serão aqueles que possibilitem ou intercetem, de certa forma, comunicações em ambiente digital. Lança, a título de exemplo: a intromissão em salas de *chat*; fóruns reservados, sempre com a finalidade de obter informações ou captar comunicações; e o envio e troca de material pornográfico ou pedo-pornográfico, para adquirir a confiança do sujeito ou dos membros de uma rede criminosa.

Alerta, ainda, para o facto de se poder alegar que esta não foi a intenção do legislador histórico. Contudo, independentemente da verdadeira vontade, entende ser claro que a formulação do n.º 2 não cumpre o princípio de reserva de lei. Este exige, por um lado, a suficiente especificação e, por outro, uma densificação.

Para SILVA DIAS, o que se encontra neste número é, desde logo, a falta de exigência da especificação. Isto porque, à luz de uma interpretação objetiva e constitucionalmente conforme, o recurso a esta fórmula vaga e indeterminada – "meios e dispositivos informáticos" –, bem como a remissão geral para um regime inadequado (interceção de comunicações), não constitui especificação suficiente para o uso de *malware*. Por fim, acautela que não podemos esquecer que esta exigência é tanto maior quanto mais intrusivo for o meio.

---

[349] Em sentido contrário, considera DAVID SILVA RAMALHO, «O uso de *malware*…», op. cit., pp. 229-230, que o agente encoberto *online* está previsto antes no n.º 1 do artigo 19.º da LC. Veja-se, ainda deste autor, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, op. cit., pp. 309-310.

Diante do exposto, observa que também se terá de considerar que o n.º 2 nem sequer prevê a possibilidade do emprego de *malware*, e que só esta conclusão garante a segurança jurídica num domínio tão compressor de direitos fundamentais.

Atendendo a tudo o que foi acima referido, e salvo melhor opinião, também concluímos que o *malware* como método oculto de investigação não se encontra previsto na LC. Afastamos, imediatamente, a possibilidade de este meio estar regulado nos artigos 15.º e 18.º da LC, aderindo, para o efeito, aos fundamentos invocados pelos autores referidos neste último subtítulo. No que diz respeito ao n.º 2 do artigo 19.º da LC, tivemos, inicialmente, algumas reticências. Todavia, perante o que expusemos no capítulo quarto e no que ora tratámos, essas dúvidas ficaram afastadas.

Quanto ao n.º 2 do artigo 19.º da LC, entendemos não estar suficientemente especificado. Por um lado, ao remeter, de modo genérico, para "meios e dispositivos informáticos", não garante um conhecimento esclarecido. Por outro, devido ao grau de danosidade do próprio método, ele não deveria estar inserido nas ações encobertas nem remeter, simplesmente, para o regime de interceção das comunicações[350]. Tal forma de redação aumenta em excesso os riscos que resultam para os destinatários desta norma, face aos poderes de atuação. Na verdade, o que ela fornece são critérios pouco claros que permitem a liberdade de escolha e a não salvaguarda do núcleo essencial dos direitos constitucionalmente protegidos. Por sua vez, não possibilita, em última instância, um controlo eficaz e objetivo da atuação da entidade que investiga com base nesta norma.

Só uma lei expressa, com clareza e determinação suficientes, que defina e delimite o âmbito deste meio, poderá legitimar o emprego de *malware* como método de obtenção de prova em processo penal. Assim, a técnica legislativa mais adequada seria, nas considerações de AUGUSTO SILVA DIAS[351], a de indicar o tipo de *software* a utilizar, de modo a que em termos claros se compreendesse que o mesmo está previsto na lei. Ou seja, o procedimento não implica a descrição detalhada de todos os dispositivos que integram o conceito de *malware* – pois levaria a que a norma, rapidamente, se encontrasse desatualizada face à vertiginosa evolução tecnológica que se verifica nos tempos modernos –, mas apenas uma descrição do tipo de *software(s)* a que se poderá recorrer.

[350] Pelo menos, da forma como o faz.
[351] Cf. "O uso de *malware* como meio de obtenção de prova", comunicação acima citada.

Por seu turno, este tipo de regime deve, com clareza e precisão, prescrever o fundamento e os limites da intromissão. Isto é, em função da gravidade que implica o uso de *malware*, além de ser a *ultima ratio* e exigir uma ponderação no caso concreto, deverá especificar, entre outros: o procedimento a adotar; definir o catálogo de crimes; a competência para a sua determinação; o prazo de duração; o âmbito subjetivo; e o tipo de dados que poderão ser recolhidos. Somente deste modo se dará a conhecer à comunidade os meios processuais à disposição da investigação criminal, bem como permitir o controlo jurisdicional efetivo dos atos dos agentes de investigação, possibilitando a sindicância da legalidade e constitucionalidade dos procedimentos adotados, a validade da prova recolhida e o cumprimento dos pressupostos objetivamente verificáveis.

Nestes termos, aderimos às conclusões de AUGUSTO SILVA DIAS[352], ou seja, defendemos que o n.º 2 do artigo 19.º da LC tem falta de previsão, de densificação legal e de critérios de proporcionalidade, no que diz respeito ao uso de *malware*. Em consequência, compromete a sua constitucionalidade na interpretação que comporta a utilização de *software* malicioso, implicando a nulidade e inutilidade da prova obtida através do recurso a este meio oculto, como determina o n.º 3 do artigo 126.º do CPP.

Assim, perfilhamos a opinião de AUGUSTO SILVA DIAS[353], segundo o qual o que se encontra previsto no n.º 2 do artigo 19.º da LC é a figura do agente encoberto *online.* Dito de outro modo, o agente encoberto que se socorre de meios informáticos para criar uma identidade fictícia e investigar *online*.

[352] Cf. *Ibidem*.
[353] Cf. *Ibidem*.

7. Proposta de regime jurídico para a utilização de *malware*

Tendo concluído, devido às razões já invocadas, pela não previsão do uso de *malware* como meio de obtenção de prova no nosso ordenamento jurídico, resta-nos expor quais os requisitos que entendemos ser necessário observar para este meio encoberto.

Em primeiro lugar, temos de salientar que o nível de danosidade deste meio implica um regime mais rigoroso, comparativamente ao dos outros métodos ocultos.

Em segundo lugar, a sua consagração legal, além de acarretar uma ponderação do legislador, efetuada aos olhos do princípio da proporcionalidade em sentido lato, também impõe uma segunda reflexão por parte do aplicador da lei, isto é, do juiz, ante uma situação determinada.

Em terceiro lugar, como vimos já nos capítulos anteriores, também devem estar presentes no regime certos vetores, nomeadamente: a invocação da excecionalidade ou do último recurso; a descrição do meio a utilizar; a necessidade de reserva do juiz; a fase do processo em que é permitido; o catálogo taxativo de crimes que legitimam o seu recurso; o catálogo limitado de sujeitos sobre os quais pode recair o método; a duração da diligência; e o procedimento aplicável.

Em síntese, os mencionados requisitos não serão meras formalidades, mas sim a garantia do respeito pelos direitos fundamentais.

7.1 Ponderação

O *malware*, por constituir um dos métodos ocultos de investigação com maior grau de dano e devassa, requer que seja utilizado apenas como último recurso. Só se poderá recorrer a este meio encoberto, se houver razões para crer que esta diligência é indispensável à descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter. Portanto, a lógica da sua utilização deve obedecer ao princípio da subsidiariedade: emprega-se este meio apenas se um outro menos lesivo não for suficiente para obter o mesmo resultado. Não basta que sem ele a investigação se torne mais difícil; é imperativo que se torne praticamente impossível[354].

Salientamos, igualmente, tal como referido a este propósito nas escutas telefónicas, que o desejado é uma ponderação baseada em hipóteses ou probabilidades

[354] Se para um método oculto menos lesivo basta que sem a medida a investigação ficasse mais difícil, aqui terá que ser praticamente impossível. Cf. MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação…», op. cit., p. 546.

dos elementos de prova que se poderiam obter com recurso ao *malware*, e que não seriam possíveis de alcançar através de outros meios menos lesivos.

Por fim, na consideração da utilização ou não de *malware*, deverá haver um reforço da ponderação dos princípios da adequação, da necessidade e da proporcionalidade. Em concreto, o juiz deve verificar se estão preenchidos os pressupostos legais para a sua utilização, se o meio é adequado ao caso, é proporcional ao fim que se pretende e à gravidade do crime que se investiga. Em suma, não basta estarmos perante um crime do catálogo. É necessário que a diligência seja apta ao resultado pretendido, proporcional à gravidade concreta do crime e exatamente necessária.

7.2 Descrição do uso de *malware*

É imprescindível que o regime jurídico faça alusão ao método oculto. Deste modo, a norma deve apresentar uma descrição simples do meio a utilizar. Significa ter de referir que se irá instalar, física ou remotamente, um dispositivo ou *software* no sistema informático que, sem conhecimento do seu utilizador e via telemática, permite aceder a dados informáticos, gravá-los, conservá-los e transmiti-los da mesma forma como se encontram armazenados no sistema, do jeito que se apresentam no ecrã para o utilizador, da maneira como eles vão sendo introduzidos, ou tal como eles são recebidos e transmitidos por dispositivos audiovisuais.

Importa alertar que o *software* malicioso deve permitir o mínimo de alterações no sistema informático do visado, bem como a sua reversão. Por outro lado, a técnica utilizada deve proteger o sistema informático visado de eventuais acessos não autorizados, através de meios semelhantes.

Também consideramos pertinente a existência de um registo oficial do *software* ou dispositivos que se podem utilizar para este método, assim como a sua revisão anual[355].

Deverá existir ainda uma lista de pessoas com formação e competência técnica para executar este método, mas sempre pertencentes aos órgãos de polícia criminal.

[355] Como está previsto no Projeto Italiano.

7.3 Fase e competência

O regime jurídico deve definir em que situações este método oculto poderá ser utilizado. Salvo melhor opinião, consideramos que ele poderá servir para obstar à continuação da atividade criminosa[356], assim como para punir a prática já consumada.

Em caso de prevenção, a autorização da medida será da incumbência do juiz do tribunal central de instrução criminal, mediante requerimento do Departamento Central de Investigação e Ação Penal, por iniciativa do magistrado do Ministério Público junto do mesmo. Já no caso de repressão criminal, competirá ao juiz de instrução criminal autorizar o recurso a este meio, mediante requerimento do Ministério Público.

O juiz de instrução deverá pronunciar-se no mais curto prazo possível acerca da utilização de *malware*, em consideração das próprias características da prova digital e a possibilidade de esta vir a 'desaparecer'. O despacho de autorização do juiz de instrução criminal deverá: indicar a pessoa visada e, caso seja possível, identificá-la com o nome e morada; descrever o *software* ou o dispositivo a instalar; traçar, o mais detalhadamente possível, o sistema informático a aceder e, sempre que se conheça, indicar a sua localização; citar os dados de recolha permitidos; mencionar o modo de acesso e apreensão dos mesmos; e indicar o âmbito da diligência e a infração em causa. O despacho deverá ainda referir quem irá executar e supervisionar o método; autorizar a realização e a conservação da cópia dos dados recolhidos; assinalar as medidas necessárias para a preservação, autenticidade, integridade, inacessibilidade ou supressão dos dados armazenados no sistema informático acedido; referir a duração do meio, com a data exata em que terminará; e fundamentar a autorização do recurso ao *malware*, estando aqui subjacente a indispensabilidade para a descoberta da verdade, ou o juízo sobre a impossibilidade ou grande dificuldade para obter prova.

Naturalmente, por razões óbvias, será importante que o Ministério Público, os órgãos de polícia criminal e o juiz de instrução criminal tenham formação adequada para o recurso a este tipo de meio oculto.

---

[356] Tendo em consideração o já alertado, a propósito das ações encobertas, por PAULO DE SOUSA MENDES**,** «Investigação, prevenção e informação de segurança», op. cit., p. 70**,** entendemos que o regime jurídico deve indicar as situações consideradas de prevenção.

7.4 Catálogo

7.4.1 Crimes

O objetivo de fixar um catálogo de crimes neste regime permite que, só quando estamos perante um deles, seja possível recorrer a este meio. Assim, todos os outros crimes estão excluídos da possibilidade de utilização de *malware*, para obtenção de prova.

Após termos analisado, no capítulo terceiro, o catálogo de crimes previsto no regime jurídico do *malware* em vários direitos estrangeiros, bem como, posteriormente, o catálogo existente no nosso ordenamento jurídico para as escutas telefónicas e as ações encobertas, chegamos a duas conclusões: (1) no direito estrangeiro (pelo menos na maioria dos casos), os crimes previstos são graves; e (2) devido ao grau danoso deste método comparativamente com as escutas e as ações encobertas, o nosso catálogo deveria prever crimes ainda mais graves[357].

Diante do exposto, somos de opinião que o catálogo taxativo de crimes para este regime jurídico deverá contemplar os seguintes: crime de tráfico e mediação de armas; crime de genocídio; crimes contra a Humanidade; crime de tráfico, branqueamento de estupefacientes e substâncias psicotrópicas, através de associação criminosa, exceto tráfico de menor gravidade; crimes cometidos por organização terrorista; crime de terrorismo; crime de terrorismo internacional; crime de financiamento ao terrorismo; crime de branqueamento de capitais e outros; e criminalidade altamente organizada[358]. Deverá incluir também a criminalidade especialmente violenta; o abuso sexual e exploração sexual de crianças e pornografia infantil[359]; os crimes contra a segurança das comunicações, a que corresponda, em abstrato, pena de prisão superior a oito anos; os crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico; e os crimes cometidos por meio de um sistema informático, quando lhe corresponda, em abstrato, pena de prisão no máximo superior a oito anos.

---

[357] Neste sentido, MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação…», op. cit., p. 545.

[358] Frise-se que na criminalidade altamente organizada, o quadro de crimes subjacentes não pode causar insegurança. A segurança só se alcança se estivermos perante definições concretas. Portanto, tem de haver uma uniformização deste conceito.

[359] Apesar das penas aplicáveis em abstrato não serem muito elevadas, consideramos que não faria sentido excluir estes crimes do catálogo, tal como nos casos que apresentámos no capítulo terceiro.

Todavia, nos casos de prevenção, consideramos que este meio só poderá ser utilizado em crimes cometidos por organização terrorista, de terrorismo e de terrorismo internacional, à semelhança do que prevê o regime jurídico alemão.

Alerta-se, contudo, que deve o regime jurídico oferecer ao intérprete critérios de determinação no caso dos crimes que por si podem ser suscetíveis de indeterminação[360].

Por último, é de salientar que tem de haver uma suspeita fundada[361] da preparação da prática de um dos crimes referidos ou mesmo a prática de um dos previstos no catálogo, ou seja, um certo nível de indícios. Por outro lado, na sua ponderação, o juiz não se deve bastar à suspeita, devendo também verificar se este meio é adequado ao caso concreto.

7.4.2 Sujeitos

Mais uma vez, o objetivo do catálogo de sujeitos é obstar a que este meio verse contra qualquer pessoa. Assim, quanto aos sujeitos, poderão ser o arguido ou o suspeito e o intermediário.

Nos termos da alínea e) do artigo 1.º do CPP, deve considerar-se suspeita a pessoa relativamente à qual exista indício de que cometeu ou se prepara para cometer um crime ou, em alternativa, nele participou ou se prepara para participar.

O intermediário, por sua vez, é aquela pessoa que pela proximidade com o suspeito ou o arguido se afigure como potencial interlocutor. Ou seja, deverá existir uma suspeita fundada de que através dele são discutidos assuntos que se prendem com o crime em investigação.

Consequentemente, é o Ministério Público que tem de provar essa qualificação, cabendo ao juiz de instrução criminal verificar apenas a sua legalidade.

Acresce que o recurso ao *malware* deve recair sobre o sistema informático em concreto que é utilizado. Não significa isto que, necessariamente, estes sujeitos sejam os proprietários; basta fazerem uso regular desse sistema.

Por fim, deverá acautelar-se a utilização deste meio oculto, quando estejam em causa comunicações entre o arguido e o seu defensor, ou entre o mesmo e as pessoas que tenham a faculdade de se recusar a depor em nome do segredo profissional.

---

[360] Já JORGE DE FIGUEIREDO DIAS, «O Processo Penal Português: Problemas e Prospectivas», op. cit., pp. 810-811, havia alertado para este problema de indeterminação em alguns regimes jurídicos de meios ocultos de obtenção de prova.

[361] Aqui, não nos podemos esquecer que o grau de suspeita tem de ser mais exigente, em comparação com aquela que é exigida para outros meios ocultos. Neste sentido, MANUEL DA COSTA ANDRADE, «Métodos ocultos de investigação…», op. cit., p. 546.

7.5 Duração

Relativamente à duração do método, concluímos que o prazo razoável seria de um mês, renovável por igual período, desde que se verifiquem os respetivos requisitos de admissibilidade, com o limite máximo de três meses[362], a partir da sua autorização.

Chegámos a tal conclusão, porquanto se as escutas telefónicas podem ser realizadas durante três meses, um meio mais compressor de direitos fundamentais e que permite a recolha de uma grande quantidade e qualidade de dados não deverá ter um prazo tão longo. Por outro lado, devido às potencialidades do uso de *malware*, será possível com maior rapidez e facilidade recolher a prova necessária, não se justificando um alargado prazo. Como vimos no capítulo terceiro, foi possível recolher a prova em poucas semanas, naquelas ações em que se recorreu a este método.

7.6 Procedimento

Quanto ao procedimento, consideramos que deverá existir um auto de início, relatórios intercalares e um relatório final.

No início da diligência, quem executa este meio encoberto terá de elaborar um auto inicial, onde conste, além da menção do despacho de autorização, a identidade da pessoa que executa o meio, as operações efetuadas para instalar o *software* ou dispositivo e as operações para capturar os dados informáticos, bem como a data e hora de início e fim.

Durante a investigação, quem executa e supervisiona o método deverá elaborar um relatório semanal onde se registe e documente todas as ações, se descreva os dados recolhidos e relevantes para a prova e se explique o seu alcance para a descoberta da verdade material. Este documento será remetido ao Ministério Público, o qual deverá dispor, por exemplo, de trinta e seis horas para se pronunciar. Posto isto, dar-se-á conhecimento do mesmo ao juiz de instrução criminal. Este deverá decidir num curto prazo, por exemplo em vinte e quatro horas, se se mantém a indispensabilidade deste meio e, se sim, em que termos. O objetivo dos relatórios intercalares será garantir o controlo do juiz de instrução relativamente à autorização e comprovar a relevâncias dos elementos recolhidos.

---

[362] Assim dispõe também o artigo 588 *septies c* da *Ley de Enjuiciamiento Criminal*. Poderá consultar o mesmo em
http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10725.

Finda a investigação, será redigido um relatório final detalhado, sem comprometer o segredo da técnica, por quem executou e supervisionou a diligência. Este relatório será junto aos autos e deve conter: o dia, a hora e o local em que foi executado o meio, e o dia e a hora em que terminou; identificar a pessoa visada; descrever o meio técnico que foi utilizado; indicar o modo de instalação; detalhar as características do sistema informático, o estado em que se encontrava e as alterações sofridas após o acesso; descrever os dados recolhidos e os essenciais para a descoberta da verdade; detalhar o modo de garantia da cadeia de custódia; e a duração desta diligência. O intuito é possibilitar ao visado o controlo da legalidade e da regularidade deste método oculto e de assegurar o exercício do contraditório.

Naturalmente, com o fim da diligência, o *malware* tem de ser eliminado com segurança do sistema informático, sendo também elaborado um relatório deste procedimento.

Quanto aos dados recolhidos, deverão ser enviados para análise de uma entidade a criar. Esta verifica os mesmos, com a colaboração do juiz de instrução. Com esta diligência, pretende-se apurar se os dados recolhidos dizem respeito ao núcleo central da vida privada. Feita a triagem, os dados que disserem respeito exclusivamente a este núcleo ou forem estranhos ao processo devem ser eliminados de imediato, elaborando-se um relatório para o efeito. Os restantes dados serão guardados pelo Ministério Público, por exemplo, em ficheiro encriptado, devendo ser eliminados num prazo razoável ou quando concluído o processo.

Considerações finais

O uso de *malware*, como meio de obtenção de prova em processo penal, não é uma novidade dos dias de hoje. Ao longo das últimas duas décadas, foram várias as circunstâncias em que se recorreu a este método, designadamente, porque os autores de crimes recorreram à criptografia ou utilizaram mecanismos de anonimização. Além desse motivo, concluímos também que este meio oculto é necessário no combate à criminalidade contemporânea, em especial: crimes cometidos por organização terrorista; crime de terrorismo; crime de terrorismo internacional; crime de financiamento ao terrorismo; e criminalidade altamente organizada que, devido às suas particularidades, dificulta a utilização de meios de obtenção de prova 'tradicionais'.

Consideramos que este método seja útil e imprescindível, devido às suas potencialidades e ao facto de permitir a recolha de uma grande quantidade e qualidade de informações/prova, face à (quase) impossibilidade dessa recolha em determinados contextos e no combate à criminalidade. No entanto, estamos conscientes de que o faz em prejuízo de um enorme leque de direitos fundamentais e princípios enraizados em processo penal.

Todavia, após termos ponderado os valores em conflito, concluímos que os direitos fundamentais à palavra, à imagem e à intimidade, bem como o direito à integridade e confidencialidade dos sistemas informáticos, devem 'ceder' à descoberta da verdade material, à realização da justiça, ao restabelecimento da paz jurídica (comunitária) e à proteção de outros direitos fundamentais.

Contudo, sem mais e simplesmente, não podemos considerar admissível esta restrição aos direitos fundamentais. Para o efeito, a mesma tem de ser acompanhada de determinados critérios, como: a reserva de lei; o princípio da proporcionalidade em sentido amplo; o princípio da subsidiariedade; e princípio da reserva do juiz. Estes definem coordenadas que irão permitir a legitimidade do uso de *malware*, como meio de obtenção de prova. Portanto, de certo modo, podem e devem ser consideradas as traves mestras na concretização do regime jurídico do *malware*.

Ora, foi precisamente ao verificarmos que os critérios acima referidos são indispensáveis na consagração deste método oculto, que acabamos por aferir que este meio de obtenção de prova, na atualidade, não está previsto no nosso ordenamento jurídico, designadamente nos artigos 15.º, 18.º e 19.º n.º 2 da LC.

Em consequência, e por causa deste método encoberto se revelar necessário e profícuo ao prosseguimento dos fins supracitados, entendemos que o legislador deverá prestar atenção às exigências que hoje se verificam e intervir através de legislação, obviamente, sem deixar de respeitar os ditames constitucionais.

Assim, de forma expressa, clara e determinada, tal como verificamos nos regimes jurídicos estrangeiros que prevêem o recurso a *software* malicioso, bem como no nosso regime das escutas telefónicas e das ações encobertas, o legislador deverá definir e delimitar o âmbito do uso de *malware*. Ou seja, o seu regime jurídico terá de ser estruturado com base nos seguintes vetores: descrição deste meio de obtenção de prova; subsidiariedade; proporcionalidade; catálogo de crimes; grau de suspeita; catálogo de sujeitos; autorização/ordenação por autoridade competente; duração; procedimento a ser observado; e informação do sujeito visado, depois de terminada a medida. Serão estes os pressupostos, cumpridos os princípios constitucionais que referimos, que legitimarão o uso deste método oculto, bem como a valoração da prova obtida através dele.

Por fim, face às críticas constantemente tecidas acerca dos meios ocultos de investigação criminal, não queremos deixar de relembrar que entendemos que o regime jurídico do *malware* deverá ser integrado no CPP. Somente, deste modo, se começarão a dirimir lacunas, descontinuidades, incongruências e inconsistências, que atualmente se verificam neste âmbito.

Bibliografia

ABEL, Wiebke, e Burkhard SCHAFER

– «The German Constitucional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822», *SCRIPTed - A Journal of Law, Technology & Society*, volume 6, número 1, abril de 2009.

ALBRECHT, Hans-Jörg

– «Vigilância das telecomunicações. Análise teórica e empírica da sua implementação», *Que Futuro Para o Direito Processual Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, coord. Mário Ferreira Monte *et al*., Coimbra: Coimbra Editora, 2009.

ALBUQUERQUE, Paulo Pinto de

– *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2.ª edição, Lisboa: Universidade Católica Editora, 2008.

– *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, 4.ª edição, Lisboa: Universidade Católica Editora, 2011.

ANDRADE, Manuel da Costa

– *"Bruscamente no Verão Passado", a reforma do Código de Processo Penal. Observações críticas sobre uma Lei que podia e devia ter sido diferente*, Coimbra: Coimbra Editora, 2009.

– «Das Escutas Telefónicas», *in* Manuel Monteiro Guedes Valente (coord.), *I Congresso de Processo Penal*, Coimbra: Almedina, 2005.

– «Métodos ocultos de investigação (*Plädoyer* para uma teoria geral)», *Que Futuro Para o Direito Processual Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, coord. Mário Ferreira Monte *et al*., Coimbra: Coimbra Editora, 2009.

BRAVO, Teresa Maria da Silva

– «Revistas e Buscas: O Processo Penal na Era da Globalização», *in* Manuel Monteiro Guedes Valente (coord.), *III Congresso de Processo Penal*, Coimbra: Almedina, 2010.

BRENNER, Susan W.

– *Cybercrime and the law, challenges, issues, and outcomes*, Boston: Northeastern University Press, 2012.

– «*At Light Speed*: Attribution and Response to Cybercrime/Terrorism/Warfare», *Journal of Criminal Law and Criminology*, volume 97, tomo 2, 2007.

BUENO DE MATA, Federico

– «El agente encubierto en la internet: mentiras virtuales para alcanzar la justicia», *in Los retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional), A Coruña, 2 y 3 de junio de 2011*, coord. Ana Neira Pena *et al.*, Corunha: Universidade de Coruña, 2012.

– «Un centinela virtual para investigar delitos cometidos a través de las redes sociales: ¿ deberían ampliarse las actuales funciones del agente encubierto en internet?», *El proceso penal en la sociedad de la información: Las nuevas tecnologías para investigar probar el delito*, coord. Julio Pérez Gil, Madrid: *La Ley*, 2012.

CAIRES, João Gouveia de

– «O registo de som e imagem e as escutas ambientais», *in Direito da Investigação Criminal e da Prova*, coord. Maria Fernanda Palma *et al*., Coimbra: Almedina, 2014.

CANOTILHO, J. J. Gomes, e Vital MOREIRA

– *Constituição da República Portuguesa Anotada*, 4.ª edição revista, volume I, Coimbra: Coimbra Editora, 2007. (2014)

CLOUGH, Jonathan

– *Principles of Cybercrime*, Cambridge: Cambridge University Press, 2010. (2.ª edição, 2015)

COMPUTER FRAUD & SECURITY

– «BadTrans is bad worm», *Computer Fraud & Security*, volume 2002, tomo 1, janeiro de 2002.

– «Magic Lantern on back of Carnivore», *Computer Fraud & Security*, volume 2002, tomo 1, janeiro de 2002.

CORREIA, João Conde

– «Prova digital: as leis que temos e a lei que devíamos ter», *Revista do Ministério Público*, número 139, ano 35, julho/setembro de 2014.

COSTA, Eduardo Maia

– «Ações encobertas (Alguns problemas, algumas sugestões)», *in* AA. VV., *Estudos em Memória do Conselheiro Artur Maurício*, org. Maria João Antunes, Coimbra: Coimbra Editora, 2014.

CUNHA, José Manuel Damião da

– «Dos meios de obtenção da prova face à autonomia técnica e táctica dos órgãos de polícia criminal», *in* Manuel Monteiro Guedes Valente (coord.), *II Congresso de Processo Penal*, Coimbra: Almedina, 2006.

– «O Regime Legal das Escutas Telefónicas – Algumas Breves Reflexões», *Revista do CEJ*, número 9 (especial), 1.º semestre de 2008.

DELGADO MARTÍN, Joaquín

– «Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos», *Diario La Ley*, número 8202, 29 de novembro de 2013.

DIAS, Augusto Silva

– «Criminalidade organizada e combate ao lucro ilícito», *in* Maria Fernanda Palma *et al*. (coord.), *2.º Congresso de Investigação Criminal*, Coimbra: Almedina, 2011.

DIAS, Jorge de Figueiredo

– «O Processo Penal Português: Problemas e Prospectivas», *Que Futuro Para o Direito Processual Penal? Simpósio em Homenagem a Jorge de Figueiredo Dias, por ocasião dos 20 anos do Código de Processo Penal Português*, coord. Mário Ferreira Monte *et al*., Coimbra: Coimbra Editora, 2009.

FERNÁNDEZ LÓPEZ, Mercedes

– «Algunas propuestas para regular la investigación del cibercrimen», *in La reforma del proceso penal*, Madrid: Editorial La Ley, 2011.

GASPAR, António da Silva Henriques *et al*.

– *Código de Processo Penal Comentado*, Coimbra: Almedina, 2014. (2.ª edição, 2016)

GLISS, Hans

– «German police and Secret Service propose use of Trojan horse: a crazy notion», *in Computer Fraud & Security*, volume 2007, tomo 4, abril de 2007.

GOUVEIA, Jorge Bacelar

– *Manual de Direito Constitucional. II - Direito Constitucional Português*, 6.ª edição revista e atualizada, Coimbra: Almedina, 2016.

HOFFMANN-RIEM, Wolfgang

– «Innovaciones en la Jurisprudencia del Tribunal Constitucional Alemán, a propósito de la garantía de los derechos fundamentales en respuesta a los cambios que conducen a la sociedad de la información», *Revista de Derecho Constitucional Europeo*, número 22, julho/dezembro de 2014 (tradução Antonio López Pina e Angelika Freund).

JESUS, Francisco Marcolino de

– *Os Meios de Obtenção da Prova em Processo Penal*, 2.ª edição revista, atualizada e ampliada, Coimbra: Almedina, 2015.

LEITE, Inês Ferreira

– «O novo regime das escutas telefónicas. Uma visão panorâmica sobre a reforma de 2007», *in Direito da Investigação Criminal e da Prova*, coord. Maria Fernanda Palma *et al*., Coimbra: Almedina, 2014.

LUMBRALES, Nuno

– «Direitos fundamentais: o direito à palavra, o direito à imagem e a prova audiovisual em processo penal», *Revista do Ministério Público do Rio Grande do Sul*, número 67, setembro/dezembro de 2010.

MANSSEN, Gerrit

– «El "Derecho fundamental a la confidencialidad e integridad de sistemas informáticos" – un aporte exitoso a la creación de derechos de libertad?», *Boletín del Instituto de Estudios Constitucionales*, número 35, janeiro/junho de 2014 (tradução Angélica María Arango Díaz).

MARCHENA GÓMEZ, Manuel

– «Proceso penal: nuevos problemas, viejas soluciones», *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, número 100, 2013.

MATA-MOUROS, Maria de Fátima

– *Juiz das Liberdades. Desconstrução de um mito do processo penal*, Coimbra: Almedina, 2011.

– «Escutas Telefónicas – O que não Muda com a Reforma», *Revista do CEJ*, número 9 (especial), 1.º semestre de 2008.

MENDES, Paulo de Sousa

– «Investigação, prevenção e informação de segurança», *in* Manuel Monteiro Guedes Valente (coord.), *IV Congresso de Processo Penal - I Congresso Luso-Brasileiro de Criminalidade Económica-Financeira*, Coimbra: Almedina, 2016.

– *Lições de Direito Processual Penal*, 3.ª reimpressão, Coimbra: Almedina, 2015.

MESQUITA, Paulo Dá

– *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Coimbra Editora (Wolters Kluwer), 2010.

MILITÃO, Renato Lopes

– «A propósito da *prova digital* no processo penal», *Revista da Ordem dos Advogados*, volume I, ano 72, janeiro/março de 2012.

MIRANDA, Jorge

– *Manual de Direito Constitucional. Direitos fundamentais*, 5.ª edição, tomo IV, Coimbra: Coimbra Editora (Wolters Kluwer), 2012.

MIRANDA, Jorge, e Rui MEDEIROS

– *Constituição Portuguesa Anotada, tomo I*, 2.ª edição, Coimbra: Coimbra Editora, 2010.

– *Constituição Portuguesa Anotada, tomo I*, Coimbra: Coimbra Editora, 2005.

MOLINA MANSILLA, M.ª del Carmen

– «El agente encubierto (artículo 282 bis de la LECrim.)», *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, número 62, julho de 2009.

MONTE, Mário Ferreira

– «Escutas Telefónicas», *in* Manuel Monteiro Guedes Valente (coord.), *III Congresso de Processo Penal*, Coimbra: Almedina, 2010.

MURPHY, Angela

– «Cracking the Code to Privacy: How Far Can the FBI Go?», *Duke Law & Technology Review*, volume 1, tomo 1, janeiro de 2002.

NEVES, Rita Castanheira

– *As Ingerências nas Comunicações Electrónicas em Processo Penal – natureza e respetivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra: Coimbra Editora (Wolters Kluwer), 2011.

NOVAIS, Jorge Reis

– *As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição*, Tese de Doutoramento em Ciências Jurídico-Políticas, Lisboa: Faculdade de Direito da Universidade de Lisboa, 2002, volume II. (policopiada)

– *As restrições aos Direitos Fundamentais não expressamente autorizadas pela Constituição*, 2.ª edição, Coimbra: Coimbra Editora, 2010.

– *Os Princípios Constitucionais Estruturantes da República Portuguesa*, Coimbra: Coimbra Editora, 2011.

ORTIZ PRADILLO, Juan Carlos

– «El *Remote Forensic Software* como Herramienta de Investigación contra el Terrorismo», *ENAC*, número 4, outubro de 2009.

– *La investigación del delito en la era digital. Los derechos fundamentales frente a las nuevas medidas tecnológicas de investigación*, Madrid: Fundación Alternativas, 2013.

– *Problemas Procesales de la Ciberdelincuencia*, Madrid: Editorial Colex, 2013.

– «*Hacking* legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delincuencia informática», *Revista de Derecho y Proceso Penal*, número 26, 2011.

OWSLEY, Brian L.

– «Beware of Government Agents Bearing Trojan Horses», *Akron Law Review*, volume 48, tomo 2, 2015.

PALMA, Maria Fernanda

– «A teoria do crime como teoria da decisão penal e o Direito da Investigação Criminal», *in Direito da Investigação Criminal e da Prova*, coord. Maria Fernanda Palma *et al*., Coimbra: Almedina, 2014.

– «Introdução ao Direito da Investigação Criminal e da Prova», *in Direito da Investigação Criminal e da Prova*, coord. Maria Fernanda Palma *et al*., Coimbra: Almedina, 2014.

– «Tutela da vida privada e processo penal – realidades e perspectivas constitucionais», *Jurisprudência Constitucional*, número 10, abril/junho de 2006, Coimbra: Coimbra Editora.

– «Tutela da vida privada e processo penal (soluções para o conflito de valores na jurisprudência constitucional)», *in Estudos em Memória do Conselheiro Luís Nunes de Almeida*, Coimbra: Coimbra Editora, 2007.

PARTNERS, XMCO

– «Les Federal Trojans», *L'ActuSécu*, número 21, 2008.

PEREIRA, António Garcia

– «Breves reflexões sobre o estado presente do Processo Penal em Portugal», *in* Manuel Monteiro Guedes Valente (coord.), *III Congresso de Processo Penal*, Coimbra: Almedina, 2010.

PEREIRA, Rui

– «O *Agente Encoberto* na Ordem Jurídica Portuguesa», *in* AA. VV., *Estudo em Homenagem ao Conselheiro José Manuel Cardoso da Costa*, volume II, Coimbra: Coimbra Editora, 2005.

PINHEIRO, Alexandre Sousa

– *Privacy e proteção de dados pessoais: a construção dogmática do direito à identidade informacional*, Lisboa: AAFDL Editora, 2015.

PINTO, Ana

– *Investigação criminal com recurso a meios telemáticos: em especial, as buscas online e o agente infiltrado online*, Dissertação de Mestrado em Direito Especialidade em Ciências Jurídico-Forenses, Lisboa: Faculdade de Direito da Universidade de Lisboa, 2015. (policopiada)

PINTO, Paulo Mota

– «A proteção da vida privada na jurisprudência do Tribunal Constitucional», *Jurisprudência Constitucional*, número 10, abril/junho de 2006, Coimbra: Coimbra Editora.

RAMALHO, David Silva

– *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Dissertação de Mestrado em Direito, Especialidade de Ciências Jurídico-Criminais, Lisboa: Faculdade de Direito da Universidade de Lisboa, 2015. (policopiada)

– «O uso de *malware* como meio de obtenção de prova em processo penal», *Revista de Concorrência e Regulação*, número 16, ano IV, outubro/dezembro de 2013.

REDONDO HERMIDA, Álvaro

– «El *agente encubierto* en la Jurisprudencia española y en la doctrina del Tribunal Europeo de Derechos Humanos», *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, número 45, janeiro de 2008.

RODRIGUES, Benjamim Silva

– *Da Prova Penal. Da Prova-Electrónico-Digital e da Criminalidade Informático-Digital*, Lisboa: Rei dos Livros, 2011.

SILVA, Daniel

– «Ações encobertas no Estado de Direito Democrático», *Investigação Criminal*, número 5, maio de 2013.

SILVA, Germano Marques da

– *Curso de Processo Penal*, 5.ª edição revista e atualizada, volume II, Lisboa: Editorial Verbo, 2011.

– «Os novos desafios do processo penal», *in* Manuel Monteiro Guedes Valente (coord.), *II Congresso de Processo Penal*, Coimbra: Almedina, 2006.

SILVEIRA, Maria Ana Barroso de Moura da

– *Da Problemática da Investigação Criminal em Ambiente Digital – em Especial, sobre a Possibilidade de Utilização de Malware como Meio Oculto de Obtenção de Prova, Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Dissertação de Mestrado, Lisboa: Universidade Católica Portuguesa, Faculdade de Direito – Escola de Lisboa, 2016. (policopiada)

TEIXEIRA, Carlos Adérito

– «Escutas Telefónicas: A Mudança de Paradigma e os Velhos e os Novos Problemas», *Revista do CEJ*, número 9 (especial), 1.º semestre de 2008.

VACIAGO, Giuseppe, e David Silva RAMALHO

– «Online searches and online surveillance: the use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings», *Digital Evidence and Electronic Signature Law Review*, volume 13, novembro de 2016.

VALENTE, Manuel Monteiro Guedes

– «Terrorismo e Processo Penal: Uma Relação Amarga (?)!» *in* Manuel Monteiro Guedes Valente (coord.), *II Congresso de Processo Penal*, Coimbra: Almedina, 2006.

VELASCO NÚÑEZ, Eloy

– «ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal», *La Ley Penal: Revista de Derecho Penal, Procesal y Penitenciario*, número 82, maio de 2011.

VERDELHO, Pedro

– «Técnica no Novo C.P.P.: Exames, Perícias e Prova Digital», *Revista do CEJ*, número 9 (especial), 1.º semestre de 2008.

***

ABAD LIÑÁN, José Manuel

– «La Policía podrá instalar un troyano en el ordenador de sospechoso», *El País*, 08 de dezembro de 2015.

CHAMPEAU, Guillaume

– «Des failles sur le mouchard informatique de la police allemande», *Numerama*, 10 de outubro de 2011.

– «La PJ pourra enfim installer des keyloggers et autres mouchards», *Numerama*, 04 de março de 2016.

– «LOPPSI: l'installation de mouchards chez les suspects est adoptée», *Numerama*, 11 de fevereiro de 2010.

COCHARD, Sandrine

– «Loppsi 2: comment le gouvernement veut-il surveiller nos ordinateurs?», *20 Minutes*, 29 de janeiro de 2014.

LAUSSON, Julien

– «Le mouchard de la police allemande vise aussi Skype, Gmail, Facebook….», *Numerama*, 10 de outubro de 2012.

LYNCH, Jennifer

– «New FBI Documents Provide Details on Government's Surveillance Spyware», *Electronic Frontier Foudation*, 29 de abril de 2011.

MCCULLAGH, Declan

– «How Far Can FBI Spying Go?», *WIRED*, 31 de julho de 2001.

POULSEN, Kevin

– «Documents: FBI Spyware Has Been Snaring Extortionists, Hackers For Years», *WIRED*, 16 de abril de 2009.

– «FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats», *WIRED*, 18 de julho de 2007.

– «Visit the Wrong Website and the FBI Could End Up In Your Computer», *WIRED*, 05 de agosto de 2014.

***

Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos

– Relatório sobre a luta contra a cibercriminalidade [2017/2068(INI)], Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos, Bruxelas: Parlamento Europeu, 25 de julho de 2017.

GUTHEIL, Mirja *et al*.
– *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, Estudo do Parlamento Europeu, Espaço de Liberdade, de Segurança e de Justiça, Bruxelas: Parlamento Europeu, 2017.

***

Acórdão do Supremo Tribunal de Justiça, de 26-03-2014 (Santos Cabral), processo n.º 15/10.0JAGRD.E2.S1.

Acórdão do Tribunal da Relação de Coimbra, de 06-04-2011 (Orlando Gonçalves), processo n.º 111/10.4JALRA-A.C1.

Acórdão do Tribunal da Relação de Coimbra, de 19-02-2014 (Olga Maurício), processo n.º 528/07.1GCVIS.C1.

Acórdão do Tribunal da Relação de Évora, de 20-01-2015 (João Gomes de Sousa), processo n.º 648/14.6GCFAR-A.E1.

Acórdão do Tribunal da Relação de Évora, de 17-03-2015 (Martins Simão), processo n.º 55/11.2GDSTC.E1.

Acórdão do Tribunal da Relação de Évora, de 07-04-2015 (Fernando Pina), processo n.º 13/15.8PAOLH-A.

Acórdão do Tribunal da Relação de Guimarães, de 29-03-2011 (Maria José Nogueira), processo n.º 735/10.0GAPTL-A.G1.

Acórdão do Tribunal da Relação de Guimarães, de 29-03-2014 (Maria Augusta), processo n.º 1680/03-2.

Acórdão do Tribunal da Relação de Lisboa, de 06-12-2007 (Almeida Cabral), processo n.º 10278/07-9.

Acórdão do Tribunal da Relação de Lisboa, de 25-05-2010 (Pedro Martins), processo n.º 281/08.1JELSB.L1-5.

Acórdão do Tribunal da Relação de Lisboa, de 10-05-2011 (Margarida Blasco), processo n.º 65/11.0JAFUN-A.L1-5.

Acórdão do Tribunal da Relação de Lisboa, de 24-09-2013 (Vieira Lamim), processo n.º 145/10.9GEALM.L2-5.

Acórdão do Tribunal da Relação de Lisboa, de 13-04-2016 (Carlos Almeida), processo n.º 2903/11.8TACSC.L1-3.

Acórdão do Tribunal da Relação do Porto, de 12-09-2012 (Alves Duarte), processo n.º 787/11.5PWPRT.P1.

Acórdão do Tribunal da Relação do Porto, de 27-02-2013, (Francisco Marcolino), processo n.º 494/09.0GAVLG.P1.

Acórdão do Tribunal da Relação do Porto, de 24-04-2013 (Fátima Furtado), processo n.º 585/11.6PAOVR.P1.

Acórdão Tribunal da Relação do Porto, de 22-05-2013 (Melo Lima), processo n.º 74/07.3PASTS.P1.

Acórdão do Tribunal da Relação do Porto, de 11-02-2015 (Neto de Moura), processo n.º 2063/14.2JAPRT-A.P1.

Acórdão do Tribunal da Relação do Porto, de 20-01-2016 (Artur Oliveira), processo n.º 1145/08.4PBMTS.P1.

Acórdão do Supremo Tribunal Espanhol, de 05-10-2017, STS 3565/2017.

Acórdão do Supremo Tribunal Espanhol, de 15-11-2007, STS 7815/2007.